Mixed graph states

Constanza Riera, Ramij Rahaman, Matthew G. Parker [*]

March 17, 2016

1 Introduction

The quantum *graph state*[1] is a pure quantum n-qubit state whose *joint stabilizer* can be written using a symmetric matrix whose elements are Pauli matrices. The Pauli matrices are:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad Y = iXZ,$$

where $i = \sqrt{-1}$. More precisely, in [1], graph states in n qubits are defined as the unique, common eigenvector in $(\mathbb{C}^2)^n$ to the set of independent commuting observables:

$$K_a = X_a Z_{\mathcal{N}_a} = X_a \prod_{b \in \mathcal{N}_a} Z_b$$

where $A_a = I \otimes I \otimes \cdots \otimes A \otimes I \otimes \cdots \otimes I$, $\mathcal{N}_a$ are the neighbours of a in the associated graph (see below), and where the eigenvalues to the observables K_a are $+1$ for all $a = 0, \ldots, n-1$. A natural generalisation is given by

$$K_a = \sigma_a Z_{\mathcal{N}_a} = \sigma_a \prod_{b \in \mathcal{N}_a} Z_b$$

where $\sigma \in \{X, Y\}$. For the *mixed graph states* of this paper we require this extra generality.

We represent a pure quantum graph state by a simple graph, hence the name *graph state*. For instance, for $n = 3$, the simple graph with vertices $V = \{0, 1, 2\}$ and edges $E = \{01, 02\}$ has an adjacency matrix $A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ and can be used to represent the pure quantum state of 3 qubits that is jointly stabilized (with eigenvalue 1) by $X \otimes Z \otimes Z$, $Z \otimes X \otimes I$, and $Z \otimes I \otimes X$. This set of $n = 3$ joint stabilizers can be written in matrix form as

---

[*]C. Riera is with Bergen University College, Norway. E-mail: csr@hib.no. M.G. Parker is with University of Bergen, Norway. E-mail: matthew@ii.uib.no. R. Rahaman is with University of Allahabad, India. E-mail: ramijrahaman@gmail.com

$$\mathcal{A} = i^{I_3 \star A} \star X^{I_3} \star Z^A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \star \begin{pmatrix} X & I & I \\ I & X & I \\ I & I & X \end{pmatrix} \star \begin{pmatrix} I & Z & Z \\ Z & I & I \\ Z & I & I \end{pmatrix} = \begin{pmatrix} X & Z & Z \\ Z & X & I \\ Z & I & X \end{pmatrix},$$

where '$\star$ is the element-wise product, I_3 is the 3×3 identity, and the connection with the adjacency matrix, A, should be clear. As another example, for $A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$, we get

$$\mathcal{A} = i^{I_3 \star A} \star X^{I_3} \star Z^A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & i & 1 \\ 1 & 1 & i \end{pmatrix} \star \begin{pmatrix} X & I & I \\ I & X & I \\ I & I & X \end{pmatrix} \star \begin{pmatrix} I & Z & Z \\ Z & Z & Z \\ Z & Z & Z \end{pmatrix} = \begin{pmatrix} X & Z & Z \\ Z & Y & Z \\ Z & Z & Y \end{pmatrix}.$$

As the system is stabilized by any of the n matrix rows, it is therefore also stabilized by any product of the rows. In general, this set of stabilizers forms a stabilizer code with 2^n elements, i.e. a stabilizer group, S. For instance, for $A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$, we have that $(X \otimes Z \otimes Z)(Z \otimes X \otimes I) = (Y \otimes Y \otimes I)$ is also a joint stabilizer of our graph state, as is $(Z \otimes I \otimes X)(X \otimes Z \otimes Z)(Z \otimes X \otimes I) = -(X \otimes Y \otimes Y)$.

Given the matrix $\mathcal{A}$ of stabilizers the implicit assumption above is that these elements are stabilizing a *pure* quantum state, i.e. that the n qubits are not entangled with an environment. Given this assumption then the rows of $\mathcal{A}$ must commute, otherwise they cannot define (stabilize) an n-qubit pure state. Let $|\psi\rangle$ be this pure state and let U be any row of $\mathcal{A}$. Then $U |\psi\rangle = |\psi\rangle$, where $|\psi\rangle$ is unique, the density matrix of the graph state is $\rho = |\psi\rangle \langle\psi|$, and $U \rho U^\dagger = \rho$.

Lemma 1 *Let $\rho = |\psi\rangle \langle\psi|$ be the density matrix of a pure graph state, and U as above. Then, as U is taken over all rows of $\mathcal{A}$, then $U \rho U^\dagger = \rho$ determines ρ uniquely up to local Pauli unitary equivalence.*

Proof. Since U is a tensor product of local Pauli matrices, $U |\psi\rangle \langle\psi| U^\dagger = |\psi\rangle \langle\psi|$ implies $U |\psi\rangle = \pm |\psi\rangle$. This means that $|\psi\rangle$ is a common eigenvector of the set of matrices, U, with eigenvalue ± 1. Let P be an n-fold tensor product of Pauli matrices. Then it is straightforward that $U P \rho P^\dagger U^\dagger = P U \rho U^\dagger P^\dagger = P \rho P^\dagger$, so $|\psi\rangle$ is defined by U up to local Pauli unitary equivalence. $\square$

The symmetric matrix $\mathcal{A}$ is completely characterised, up to, but not including, commutation, by $\mathcal{A}_4 = A + \omega I_n$, where $\mathcal{A}_4$ is an additive matrix over $\mathbb{F}_4$, I_n is the $n \times n$ identity matrix, ω is a primitive generator of $\mathbb{F}_4$, i.e. $\omega^3 = 1$, and where $I \to 0$, $Z \to 1$, $X \to \omega$, $Y \to \omega^2$. For instance, for $A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$, $\mathcal{A}_4 = \begin{pmatrix} \omega & 1 & 1 \\ 1 & \omega^2 & 1 \\ 1 & 1 & \omega^2 \end{pmatrix}$. The set of 2^n stabilizers then become the set of 2^n codewords of an $\mathbb{F}_4$ additive code (where multiplication of rows of $\mathcal{A}$ becomes $\mathbb{F}_4$ addition of rows of $\mathcal{A}_4$). This code is self-dual with respect to the Hermitian inner product because the matrix is symmetric with ω or ω^2 on the diagonal. Observe, however, that this map from stabilizers to $\mathbb{F}_4$ does not take into account matrix

commutation as it does not capture the minus sign of, for instance, $XZ = -ZX$, as this translates to $w.1 = 1.w$.

In this paper we define and characterise mixed graph states, by considering square matrices $\mathcal{A}$ that are not, in general, symmetric. In previous work [3] the resulting $\mathbb{F}_4$-additive codes (not, in general, self-dual) have been classified and referred to as *directed graph codes*. For instance, the adjacency matrix $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ is not symmetric and describes a mixed graph [1] comprising an undirected edge 12, and a directed edge $0 \to 1$.

As before we can map such a matrix to a matrix of stabilizers, thus:

$$\mathcal{A} = \begin{pmatrix} X & Z & I \\ I & X & Z \\ I & Z & X \end{pmatrix}.$$

But what is a natural quantum interpretation of such a matrix? Rows 0 and 2, and 1 and 2 commute, but rows 0 and 1 anti-commute. A quantum interpretation is only possible if all rows pairwise commute, so we choose to extend the rows by extra columns until the rows pairwise commute. Implicit in this column extension choice is the assumption that we add environmental qubits as opposed to, more generally, qudits or continuous variables.

In this paper we show how such matrices can define a class of mixed states, which we call *mixed graph states*. The products of the rows of the matrix still form a group, S, up to a global constant, but now the group does not have a joint eigenvector, i.e. we don't have a pure state, since some of the rows anti-commute.

Due to anti-commutativity, some of the elements of the group are only defined up to a global constant of ± 1 (there is no natural ordering on the rows of $\mathcal{A}$). For instance, for the matrix $\mathcal{A}$ associated with our example above, $(X \otimes Z \otimes I)(I \otimes X \otimes Z) = -(I \otimes X \otimes Z)(X \otimes Z \otimes I)$, as the two rows anti-commute. So S contains $\pm i(X \otimes Y \otimes Z)$.

We can than define a density matrix, ρ, which is stabilized by all members of S. Specifically,

$$s\rho s^{\dagger} = \rho \qquad \forall s \in S.$$

More generally, ρ is stabilized by any αs, where $|\alpha| = 1$, which is why we don't have to concern ourselves with global phase constants in members of S.

Throughout this paper we define the pure state vectors using a Boolean function notation [5]. Specifically, we associate with our n-qubit graph state an n-variable homogeneous generalised quadratic Boolean function $p : \mathbb{F}_2^n \to \mathbb{Z}_4$, where $p(x_0, x_1, \ldots, x_{n-1}) = \sum_{j<k} 2A_{jk}x_j x_k + \sum_j A_{jj}x_j$, and A is the modified adjacency matrix of our graph state with

---

[1] A *mixed graph* is a graph where some of the edges may be directed. In contrast, all edges of a *directed graph* are directed.

elements A_{jk}, defined as $A_{jk} = \begin{cases} \Gamma_{jk} & , j \neq k \\ 0 & , j = k \text{ and } \sigma_j = X \\ 1 & , j = k \text{ and } \sigma_j = Y \end{cases}$, with Γ the adjacency matrix of the graph. Then one can write the graph state $|\psi\rangle$ as $|\psi\rangle = 2^{-\frac{n}{2}} i^p$.

In later sections, we refer to the nodes where $\sigma_j = X$ as white nodes, and to the nodes where $\sigma_j = Y$ as red nodes.

Example 1 *We show here the mixed graph state associated with the directed triangle:*
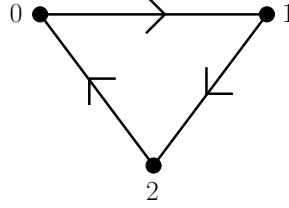
The stabilizer group S is generated, up to ± 1 constants, by:

$$X \otimes Z \otimes I$$
$$I \otimes X \otimes Z$$
$$Z \otimes I \otimes X$$

Because some of the rows of $\mathcal{A}$ anti-commute, instead of commute, there is no pure quantum state $|\psi\rangle$ such that $(X \otimes Z \otimes I) |\psi\rangle = (I \otimes X \otimes Z) |\psi\rangle = (Z \otimes I \otimes X) |\psi\rangle = |\psi\rangle$.

Instead we can associate S with the mixed graph state whose density matrix is:

$$\rho_0 = \frac{1}{8} \begin{pmatrix} 1 & 0 & 0 & i & 1 & 0 & 0 & -i \\ 0 & 1 & i & 0 & 0 & -1 & i & 0 \\ 0 & -i & 1 & 0 & 0 & i & 1 & 0 \\ -i & 0 & 0 & 1 & -i & 0 & 0 & -1 \\ 1 & 0 & 0 & i & 1 & 0 & 0 & -i \\ 0 & -1 & -i & 0 & 0 & 1 & -i & 0 \\ 0 & -i & 1 & 0 & 0 & i & 1 & 0 \\ i & 0 & 0 & -1 & i & 0 & 0 & 1 \end{pmatrix}.$$

We will discuss in later sections how we obtain this density matrix. It is easy to check that

$$(X \otimes Z \otimes I)\rho_0(X \otimes Z \otimes I)^\dagger = (I \otimes X \otimes Z)\rho_0(I \otimes X \otimes Z)^\dagger = (Z \otimes I \otimes X)\rho_0(Z \otimes I \otimes X)^\dagger = \rho_0.$$

ρ_0 is not the unique mixed graph state associated with S, however: Other density matrices ρ_j such that

$$(X \otimes Z \otimes I)\rho_j(X \otimes Z \otimes I)^\dagger = (I \otimes X \otimes Z)\rho_j(I \otimes X \otimes Z)^\dagger = (Z \otimes I \otimes X)\rho_j(Z \otimes I \otimes X)^\dagger = \rho_j$$

are:

$$\rho_1 = \frac{1}{8} \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & i & 0 & -i \\ 0 & 1 & 0 & 1 & -i & 0 & i & 0 \\ 1 & 0 & 1 & 0 & 0 & i & 0 & -i \\ 0 & 1 & 0 & 1 & -i & 0 & i & 0 \\ 0 & i & 0 & i & 1 & 0 & -1 & 0 \\ -i & 0 & -i & 0 & 0 & 1 & 0 & -1 \\ 0 & -i & 0 & -i & -1 & 0 & 1 & 0 \\ i & 0 & i & 0 & 0 & -1 & 0 & 1 \end{pmatrix}, \rho_2 = \frac{1}{8} \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & i & -i \\ 1 & 1 & 0 & 0 & 0 & 0 & i & -i \\ 0 & 0 & 1 & -1 & i & i & 0 & 0 \\ 0 & 0 & -1 & 1 & -i & -i & 0 & 0 \\ 0 & 0 & -i & i & 1 & 1 & 0 & 0 \\ 0 & 0 & -i & i & 1 & 1 & 0 & 0 \\ -i & -i & 0 & 0 & 0 & 0 & 1 & -1 \\ i & i & 0 & 0 & 0 & 0 & -1 & 1 \end{pmatrix}$$

There are also another 3 matrices which are locally equivalent to these 3 (see lemma 24). Thus we define the mixed graph state associated to the graph as

$$\rho = \sum_{i=0}^{5} c_j \rho_j$$

where $c_j \geq 0$, $\sum_{j=0}^{5} c_j = 1$, i.e. the convex sum of these density matrices. Note that, although only at most 3 of them are locally inequivalent, we include them all in the general sum ρ, since changing ρ_j for a locally equivalent ρ'_j does not necessarily give local equivalence in ρ.

Each of the ρ_j can be associated with a pure graph state in 4 qubits. For instance

$$\rho_0 = \frac{1}{2} \left| i^{2(x_0x_2+x_1x_2)+x_2} \right\rangle \left\langle i^{2(x_0x_2+x_1x_2)+x_2} \right| + \frac{1}{2} \left| i^{2(x_0x_2+x_1x_2+x_1+x_2)+x_2} \right\rangle \left\langle i^{2(x_0x_2+x_1x_2+x_1+x_2)+x_2} \right|$$

is the density matrix resulting from a measurement of qubit 3 of the pure graph state $i^{2(x_0x_2+x_1x_2+x_1x_3+x_2x_3)+x_2}$ (in terms of Boolean functions, this would correspond to the evaluation of x_3 at 0 and 1). Similarly, ρ_1 and ρ_2 are the density matrices resulting from a measurement of qubit 3 of the pure graph states $i^{2(x_0x_1+x_0x_3+x_2x_3+x_0)+x_2}$ and $i^{2(x_0x_1+x_1x_2+x_0x_3+x_1x_3)+x_1}$, while the remaining ρ_j will be given by the addition of linear terms to the polynomial.

2 Mixed graph states

To recap, a matrix such as $\mathcal{A} = \begin{pmatrix} X & Z & I \\ I & X & Z \\ I & Z & X \end{pmatrix}$ has rows that are not fully pairwise commuting, but can still be interpreted as a quantum object by making it part of a larger fully commuting matrix, i.e. where we choose the environment appropriately, and this will imply that our quantum object is a mixed state, in fact a *mixed graph state* (in this paper, we limit our study to the addition of environmental qubits as opposed to, more generally, qudits).

Let G be the mixed graph defined by adjacency matrix A, and G_b the undirected graph that has adjacency matrix $\Gamma = A + A^T$. Thus G_b is the simple graph obtained from G by erasing all undirected edges of G and making all directed edges of G undirected.

What is the minimum number of columns, e, necessary to append to $\mathcal{A}$ so as to make all rows pairwise commute? We can then add the same number, e, of rows to the matrix so as to make it square again, making sure that all resultant rows pairwise commute with the previous rows and with each other. For instance, we can extend our example by $e = 1$ columns and rows to get $\mathcal{A}' = \begin{pmatrix} & & & Z \\ & \mathcal{A} & & X \\ & & & I \\ Z & I & I & X \end{pmatrix} = \begin{pmatrix} X & Z & I & Z \\ I & X & Z & X \\ I & Z & X & I \\ Z & I & I & X \end{pmatrix}$, which is fully commuting. So for this example the minimum number of columns and rows necessary to make the matrix fully commuting was $e = 1$. Finally, as this matrix is fully commuting we can, by suitable row multiplications, recover its graph form $\mathcal{A}^e = \begin{pmatrix} X & Z & I & Z \\ Z & X & Z & I \\ I & Z & X & I \\ Z & I & I & X \end{pmatrix}$.

We consider the pure graph state described by $\mathcal{A}^e$ to be a *parent* graph state, being a parent of the mixed graph state described by $\mathcal{A}$. We then denote the resultant mixed state given by tracing out the environmental qubits as its *child*.

For our example, $\mathcal{A} = \begin{pmatrix} X & Z & I \\ I & X & Z \\ I & Z & X \end{pmatrix}$, we have $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, and the minimum number of columns and rows necessary to add to $\mathcal{A}$ to make it fully commuting is

$$e = \frac{1}{2}\text{rank}(\Gamma) = \frac{1}{2}\text{rank}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = 1$$

In general:

Lemma 2 (special case of [4]) *The minimum number, e, of columns and rows required to be added to $\mathcal{A}$ to make its rows pairwise fully commuting is given by*

$$e = \frac{1}{2}rank(\Gamma). \tag{1}$$

We refer to e as the mixed rank.

For our example we extended to a 4-qubit pure graph parent state where the 4th qubit is part of the environment. This pure graph state can be written using Boolean function notation as

$$|\psi\rangle_e = \frac{1}{4}(-1)^{x_0 x_1 + x_0 x_3 + x_1 x_2} = \frac{1}{4}(1,1,1,-1,1,1,-1,1,1,-1,1,1,1,-1,-1,-1)^T.$$

Tracing out the 4th qubit, means summing the projectors obtained by fixing $x_3 = 0$ and 1, respectively. We obtain the projectors $|\phi_0\rangle\langle\phi_0|$ and $|\phi_1\rangle\langle\phi_1|$, where $|\phi_0\rangle = \frac{1}{\sqrt{8}}(-1)^{x_0 x_1 + x_1 x_2}$,

$|\phi_1\rangle = \frac{1}{\sqrt{8}}(-1)^{x_0 x_1 + x_1 x_2 + x_0}$, and

$$\rho = |\phi_0\rangle\langle\phi_0| + |\phi_1\rangle\langle\phi_1|$$

$$= \frac{1}{8}\left\{\begin{pmatrix} 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\ -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\ -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \end{pmatrix} + \frac{1}{8}\begin{pmatrix} 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\ -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\ -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \end{pmatrix}\right\}$$

$$= \frac{1}{4}\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & -1 & 0 \\ 0 & -1 & 0 & 1 & 0 & -1 & 0 & -1 \\ 1 & 0 & 1 & 0 & 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 1 & 0 & 1 \\ -1 & 0 & -1 & 0 & -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

So we can interpret the stabilizer matrix $\mathcal{A}$ as representing the mixed quantum state ρ. However this is not a complete interpretation for two reasons:

- One can extend by more than one column/row and still obtain a fully commuting matrix.

- The matrix $\mathcal{A}$ can be extended in multiple ways, leading to multiple, possibly inequivalent, mixed states ρ.

We shall, initially, avoid the first issue by stipulating that we only extend by the minimum possible number, e, of columns/rows, as given by (1). This is compatible with the pure graph state formulation as $e = 0$ forces the state to be pure. As an example of the second issue, observe that it is equally valid to extend $\mathcal{A}$ to $\mathcal{A}' = \begin{pmatrix} & & & X \\ & \mathcal{A} & & Z \\ & & & I \\ I & Z & I & X \end{pmatrix} = \begin{pmatrix} X & Z & I & X \\ I & X & Z & Z \\ I & Z & X & I \\ I & Z & I & X \end{pmatrix}$

from which, by multiplicative row operations, we obtain $\mathcal{A}^e = \begin{pmatrix} X & I & I & I \\ I & X & Z & Z \\ I & Z & X & I \\ I & Z & I & X \end{pmatrix}$. It is

clear (since the former is a connected graph and the latter is not) that the parent graph state described by this $\mathcal{A}^e$ is locally inequivalent to the previous parent. Therefore the resultant mixed state, $\rho = |\phi_0\rangle\langle\phi_0| + |\phi_1\rangle\langle\phi_1|$, obtained by tracing out the 4th qubit, is different from the previous mixed state. In general we shall have multiple parent graph states leading to multiple density matrices, so our overall density matrix shall be a convex sum of these density matrices.

Define the *codespace* (i.e. the stabilizer group S) of the $n \times n$ matrix, $\mathcal{A}$, to be the 2^n stabilizers formed by products of one or more of the rows of $\mathcal{A}$ - remember that, as some of the rows of $\mathcal{A}$ anti-commute, some of the members of S are only defined up to a global multiplicative constant of ± 1. Likewise, the codespace of $\mathcal{A}^e$ comprises 2^{n+e} stabilizers, but now all rows of $\mathcal{A}^e$ commute so the global constant is always 1.

We refer to $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ as the *Hadamard* matrix, and to $N = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$ as the *negaHadamard* matrix. Both are unitary.

Lemma 3 *The Pauli group, $\{I, X, Z, Y\}$, is conjugated (up to a factor of ± 1) by the group generated by $\{I, H, N\}$. Specifically,*

	I	H	N	N^2	NH	HN
X	X	Z	$-Y$	Z	X	Y
Z	Z	X	X	$-Y$	$-Y$	Z
Y	Y	$-Y$	$-Z$	$-X$	Z	$-X$

For instance, $X = HZH^{\dagger}$, $-Z = NYN^{\dagger}$, and $-X = N^2Y(N^2)^{\dagger}$. Lemma 3 implies that, by conjugation, to within a factor of ± 1, we can permute the elements of the stabilizer matrix, column-wise. There are $3! = 6$ such permutations.

The following is well known (proof omitted):

Lemma 4 *Consider a quantum system comprising a local system, L, possibly entangled with an environment, E, and let ρ_L be the density matrix that defines the local system. Then unitary conjugation, $U_E(L \times E)U_E^{\dagger}$, on the environment leaves ρ_L unchanged.*

Lemma 5 *The extension columns and rows do not depend on the direction of the arrows, although the parent graphs depend on the direction of the arrows.*

Proof. The extension columns and rows depend exclusively on the commutativity or anti-commutativity of the stabiliser basis, which is not dependent on arrow direction. $\square$

3   General Density Matrix Stabilized by $\mathcal{A}$

A density matrix of n qubits can be written in a Pauli basis, i.e. where the basis elements are tensor products of elements from $\{I, X, Y, Z\}$, i.e.

$$\rho = \sum_{k \in \mathbb{Z}_4^n} a_k \tilde{\sigma}_k, \quad \text{where } k = (k_0, k_1, \ldots, k_{n-1}) \in \mathbb{Z}_4^n, \tilde{\sigma}_k = \bigotimes_{j=0}^{n-1} \sigma_{k_j}, \tag{2}$$
$$\sigma_0 = I, \sigma_1 = X, \sigma_2 = Y, \sigma_3 = Z, \text{ and } \sum_{k \in \mathbb{Z}_4^n} |a_k|^2 \leq 1,$$

where the a_k are real. Necessary and sufficient conditions for ρ to be a density matrix, i.e. derived from a statistical sum of pure states by tracing out the environment, are:

- ρ is Hermitian (i.e. equal to its transpose conjugate).

- ρ is positive semi-definite.

- $\text{Tr}(\rho) = 1$.

We refer to $\mathbf{P} = \{\tilde{\sigma}_k \mid k \in \mathbb{Z}_4^n\}$, as the set of Pauli codewords (stabilizers) of size $|\mathbf{P}| = 4^n$. Let $\mathcal{A}$ be the $n \times n$ matrix for a mixed graph state. Then $\mathcal{A}^T$ is the matrix for the mixed graph state obtained from the graph for $\mathcal{A}$ by reversing all arrows. As before, we say that $\mathcal{A}$ generates a Pauli subgroup, $S \subset \mathbf{P}$. We will now show that $\mathcal{A}^T$ generates the dual group of S, namely $S^\perp \subset \mathbf{P}$.

Theorem 1 *The set of length-n Pauli words (stabilizers) that commute with all rows of $\mathcal{A}$ forms a multiplicative group, $S^\perp$, of size 2^n, being precisely the words generated by $\mathcal{A}^T$, to within ± 1 constants.*

Proof. It is straightforward to show that every row of $\mathcal{A}^T$ commutes with every row of $\mathcal{A}$. To show that there are no more, observe that each row of $\mathcal{A}^T$ can be viewed as a restriction. Only $4^n/2^1$ (i.e. half) of all possible length-n Pauli words commute with a given row. The rows of $\mathcal{A}^T$ are independent so the n rows of $\mathcal{A}^T$ jointly commute with only $4^n/2^n = 2^n$ Pauli words. But the rows of $\mathcal{A}^T$ generate 2^n words, which must be distinct and, therefore, must be all of them. $\square$

See section 7 for a discussion of the ± 1 coefficients.

Graph states can be also described as the sum of its stabilisers, as seen in [**?**]. In order to state a similar result for mixed graph state, we need the following lemmas:

By the support of a matrix, M, we mean the set of non-zero element positions of M, i.e. $\text{support}(M) = \{(i,j)|M_{i,j} \neq 0\}$.

Lemma 6 *The elements of the stabilizer group, $S^\perp$, of a mixed graph have non-intersecting support.*

Proof. By inspection X and Y have the same support, as do I and Z. But the support of X and Y is non-intersecting with that of I and Z. Moreover if two matrices $\tilde{\sigma}_k$ and $\tilde{\sigma}_{k'}$ are both tensor products of Pauli matrices, and if they differ in at least one tensor position, where one matrix has X or Y, and the other matrix has I or Z, then $\tilde{\sigma}_k$ and $\tilde{\sigma}_{k'}$ must also have non-intersecting support. The matrix $\mathcal{A}$ only has X and/or Y on the diagonal and I and/or Z off the diagonal. Let $\mathcal{A}$ have rows numbered 0 to $n-1$. Let R and R' be two subsets of $\{0, 1, \ldots, n-1\}$ and consider the matrices, $\tilde{\sigma}_{k_R}$ and $\tilde{\sigma}_{k_{R'}}$, being the product of the rows of $\mathcal{A}$ indexed by R and R', respectively. Then $\tilde{\sigma}_{k_R}$ and $\tilde{\sigma}_{k_{R'}}$ have X or Y at tensor positions indexed by R and R', respectively, and I or Z at all other positions. So, unless R and R' are equal, they must be non-intersecting in at least one tensor position, so therefore $\tilde{\sigma}_{k_R}$ and $\tilde{\sigma}_{k_{R'}}$ have non-intersecting support. The elements of the stabilizer group of the mixed graph are obtained by ranging R over all subsets, i.e. over all stabilizer codewords. Therefore any two of them must be non-intersecting. $\square$

For a given stabilizer group S, the condition $s\rho s^\dagger = \rho \ \forall s \in S$ is equivalent to the condition $s\rho = \rho s \ \forall s \in S$. The Pauli basis description of (2) imposes the condition that $\rho = \sum_k a_k \tilde{\sigma}_k$, where the $\tilde{\sigma}_k$ are tensor products of Pauli matrices, such that $s\tilde{\sigma}_k = \tilde{\sigma}_k s \ \forall s \in S$. In other

words, ρ is the sum of tensors of Pauli matrices that commute with all $s \in S$. By theorem 1, the Pauli subgroup of matrices that commute with all elements in the stabilizer group S is the stabilizer group, $S^\perp$, of the mixed graph with the arrows reversed. The intersection of S and $S^\perp$ is then the row space of $\mathcal{A}$ associated with the vertices of the mixed graph, G, that are isolated in G_b. But what choices do we have for the angle of a_k in (2), such that ρ is also Hermitian (as a density matrix must be)? Let $a_k = \hat{a}_k \bar{a}_k$ such that $|\hat{a}_k| = 1$ and $\bar{a}_k$ is real. Lemma 6 implies that each component $a_k \tilde{\sigma}_k$ of ρ must, itself, be Hermitian, so this fixes $\hat{a}_k$ precisely, to within ± 1. For example, consider $\mathcal{A}^\perp = \begin{pmatrix} X & Z \\ I & X \end{pmatrix}$. Then $S^\perp$ contains

$$\tilde{\sigma}_{12} = \pm i (X \otimes Y) = \pm \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}, \text{ which is not Hermitian, so we choose } \hat{a}_{12} = i \text{ or}$$

$\hat{a}_{12} = -i$ in this case. In the sequel we deal with subgroups, S and $S^\perp$, of the tensored Pauli group, of size 2^n (to within ± 1 coefficients). So instead of indexing by $k \in \mathbb{Z}_4^n$, we index using $K \subset \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ relative to the rows of the group generating matrices $\mathcal{A}$ and $\mathcal{A}^T$, respectively. Specifically,

$$\rho = \sum_{k \in \mathbb{Z}_4^n} a_k \tilde{\sigma}_k = \frac{1}{2^n} \sum_{K \subset \mathbb{Z}_n} b_K \mathcal{A}_K^T, \qquad \sum_{K \subset \mathbb{Z}_n} |b_K|^2 \leq 1, \qquad \mathcal{A}_K^T \in S^\perp,$$

where the $b_K \in \{\pm 1, \pm i\}$, and $\mathcal{A}_K^T = \prod_{h \in K} \mathcal{A}_h^T$, where $\mathcal{A}_h^T$ is the hth row of $\mathcal{A}^T$, and $\prod_{h \in \{j, j'\}} \mathcal{A}_h^T = \mathcal{A}_{j'}^T \mathcal{A}_j^T$ if $j' > j$, i.e. we fix the product ordering with lowest indices on the right. Moreover, for V obtained from A^T, b_K is unique if the elements in K are pairwise commutative, and is otherwise only defined up to ± 1. For instance, if $K = \{2, 4, 5\}$ then $\prod_{h \in K} \mathcal{A}_h^T = \mathcal{A}_5^T \mathcal{A}_4^T \mathcal{A}_2^T$, and b_K is unique only if the elements in $\{2, 4, 5\}$ are pairwise commutative.

4   The maximum commutative subgroups of $S^\perp$

We now show that any commutative subgroup of the group of operators generated by the rows of $\mathcal{A}^\perp = \mathcal{A}^T$ is contained in a commutative subgroup of maximum size 2^{n-e}. Firstly, we show how the commutativity of the Pauli operators of a mixed graph state can be expressed in terms of the associated simple undirected graph, G_b, and its corresponding adjacency matrix, $\Gamma = \Gamma_{G_b}$. Then, in section 5, we show that the density matrix of any child of a pure graph state parent can be represented as a weighted sum of the terms of a maximal commutative subgroup of $S^\perp$.

Lemma 7 *Let $\mathcal{A}_j^\perp$ be row j of $\mathcal{A}^\perp$. Let $J, K \subset \{0, 1, \ldots, n-1\}$. Then $\mathcal{A}_j^\perp$ commutes with $\mathcal{A}_K^\perp$ iff the number of elements of $K \cap \mathcal{N}_j$ is even. Furthermore, $\mathcal{A}_J^\perp$ commutes with $\mathcal{A}_K^\perp$ iff the sum over J of the number of elements of $K \cap \mathcal{N}_j$ is even.*

10

Proof. $\mathcal{A}_j^\perp$ anticommutes with any $\mathcal{A}_k^\perp$ such that $k \in K \cap \mathcal{N}_j$, that is, any k in the neighbourhood of j, thus $\mathcal{A}_j^\perp \mathcal{A}_k^\perp = -\mathcal{A}_k^\perp \mathcal{A}_j^\perp$. If there are an even number of neighbours then the minus signs cancel each other out so that $\mathcal{A}_j^\perp$ commutes with $\mathcal{A}_K^\perp$, otherwise $\mathcal{A}_j^\perp$ anticommutes with $\mathcal{A}_K^\perp$. More generally, $\mathcal{A}_J^\perp$ commutes with $\mathcal{A}_K^\perp$ iff, after passing, for all $j \in J$, $\mathcal{A}_j^\perp$ through $\mathcal{A}_K^\perp$, an even number of minus signs are generated. otherwise $\mathcal{A}_J^\perp$ anticommutes with $\mathcal{A}_K^\perp$. $\qquad\square$

Example 2 *Let G_b be the simple graph 01,04,12,23,34,14. Then $\mathcal{A}_0^\perp$ commutes with $\mathcal{A}_3^\perp$ (since they are independent, so the intersection is empty), and both commute with $\mathcal{A}_K^\perp = \mathcal{A}_{\{1,2,4\}}^\perp = \mathcal{A}_4^\perp \mathcal{A}_2^\perp \mathcal{A}_1^\perp$, since 0 has 1 and 4 as neighbours, and 3 has 2 and 4 as neighbours, so both have two elements in the intersection with $K = \{1, 2, 4\}$. Note that e.g. $\mathcal{A}_0^\perp(\mathcal{A}_4^\perp \mathcal{A}_2^\perp \mathcal{A}_1^\perp) = -\mathcal{A}_4^\perp \mathcal{A}_0^\perp \mathcal{A}_2^\perp \mathcal{A}_1^\perp = -\mathcal{A}_4^\perp \mathcal{A}_2^\perp \mathcal{A}_0^\perp \mathcal{A}_1^\perp = +\mathcal{A}_4^\perp \mathcal{A}_2^\perp \mathcal{A}_1^\perp \mathcal{A}_0^\perp$. We also have that $\mathcal{A}_3^\perp \mathcal{A}_2^\perp$ commutes with $\mathcal{A}_4^\perp \mathcal{A}_1^\perp \mathcal{A}_0^\perp$, since both 2 and 3 have one neighbour in $K = \{0, 1, 4\}$, so the sum over $J = \{2, 3\}$ is even.*

Let $\Gamma_{k,j}$ be the (k, j)th element of $\Gamma = A + A^T$.

Lemma 8 *$\mathcal{A}_j^\perp$ commutes with $\mathcal{A}_K^\perp$ iff $\bigoplus_{k \in K} \Gamma_{k,j} = 0$, where $'\oplus'$ is the binary sum. Furthermore, $\mathcal{A}_J^\perp$ commutes with $\mathcal{A}_K^\perp$ iff $\bigoplus_{j \in J} \bigoplus_{k \in K} \Gamma_{k,j} = 0$. Let $v_K = (v_0, v_1, \ldots, v_{n-1}) \in F_2^n$ be such that $v_k = 1$ if $k \in K$ and $v_k = 0$ otherwise. Then the property that $\mathcal{A}_J^\perp$ commutes with $\mathcal{A}_K^\perp$ translates to the condition $v_K \Gamma v_J^T = 0$.*

Proof. We first prove that $\mathcal{A}_j^\perp$ commutes with $\mathcal{A}_K^\perp$ iff $\bigoplus_K \Gamma_{k,j} = 0$: By lemma 7, $\mathcal{A}_j^\perp$ commutes with $\mathcal{A}_K^\perp \Leftrightarrow$ the number of elements of $K \cap \mathcal{N}_j$ is even, i.e. there are an even number of rows $k \in K$ with $\Gamma_{k,j} = 1$, i.e. $\bigoplus_K \Gamma_{k,j} = 0$. Now we prove that $\mathcal{A}_J^\perp$ commutes with $\mathcal{A}_K^\perp$ iff $\bigoplus_{j \in J} \bigoplus_{k \in K} \Gamma_{k,j} = 0$: By lemma 7, $\mathcal{A}_J^\perp$ commutes with $\mathcal{A}_K^\perp$ iff the sum over J of the number of elements of $K \cap \mathcal{N}_j$ is even, i.e. there are an even number of rows $k \in K$ such that $\Gamma_{k,j} = 1$, i.e. $\bigoplus_{j \in J} \bigoplus_{k \in K} \Gamma_{k,j} = 0$. Finally, note that $v_K \Gamma = (\bigoplus_{k \in K} \Gamma_{k,0}, \bigoplus_{k \in K} \Gamma_{k,1}, \ldots, \bigoplus_{k \in K} \Gamma_{k,n-1})$, from which it follows that $v_K \Gamma v_J^T = \bigoplus_{j \in J} \bigoplus_{k \in K} \Gamma_{k,j}$. $\qquad\square$

As Γ is symmetric, we get that $v_K \Gamma v_J^T = v_J \Gamma v_K^T = 0$, which ensures that commutativity is a symmetric relationship.

Example 3 *For $\Gamma = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix}$, $\mathcal{A}_0^\perp$ commutes with $\mathcal{A}_3^\perp$ since $\Gamma_{3,0} = 0$, and both*
$\mathcal{A}_0^\perp$ *and* $\mathcal{A}_3^\perp$ *commute with* $\mathcal{A}_4^\perp \mathcal{A}_2^\perp \mathcal{A}_1^\perp$*, since $\bigoplus_{\{1,2,4\}} \Gamma_{k,0} = 1 \oplus 0 \oplus 1 = 0$ and $\bigoplus_{\{1,2,4\}} \Gamma_{k,3} = 0 \oplus 1 \oplus 1 = 0$. We also have that $\mathcal{A}_3^\perp \mathcal{A}_2^\perp$ commutes with $\mathcal{A}_4^\perp \mathcal{A}_1^\perp \mathcal{A}_0^\perp$, since $\bigoplus_{j \in \{2,3\}} \bigoplus_{k \in \{0,1,4\}} \Gamma_{k,j} = (0 \oplus 1 \oplus 0) \oplus (0 \oplus 0 \oplus 1) = 0$, i.e. $v_K \Gamma v_J^T = 0$, for $v_K = (1, 1, 0, 0, 1)$ and $v_J = (0, 0, 1, 1, 0)$.*

If $\mathcal{A}_J^\perp$ commutes with $\mathcal{A}_K^\perp$ and $\mathcal{A}_{J'}^\perp$ commutes with $\mathcal{A}_K^\perp$, and $J \cap J' = \emptyset$, then $\mathcal{A}_J^\perp \mathcal{A}_{J'}^\perp$ commutes with $\mathcal{A}_K^\perp$. Similarly, if $\mathcal{A}_J^\perp$ anti-commutes with $\mathcal{A}_K^\perp$ and $\mathcal{A}_{J'}^\perp$ anti-commutes with

$\mathcal{A}_K^\perp$, and $J \cap J' = \emptyset$, then $\mathcal{A}_J^\perp \mathcal{A}_{J'}^\perp$ commutes with $\mathcal{A}_K^\perp$. If one of them commutes and the other anti-commutes, we get anti-commutativity. This implies that subgroups can be combined to generate other subgroups in an easy way.

Lemma 9 *The subgroup structure of $S^\perp$ (and therefore also of S) is independent of the direction of the arrows in G: those graphs, G, sharing the same G_b will have the same commutative subgroup structure (although the precise group members differ).*

Proof. The subgroup structure is only dependent on G_b, which is the same regardless of arrow direction. □

From lemma 19, any two vectors $v, v' \in \mathbb{F}_2^n$ that satisfy $v\Gamma v'^T = 0$ define two commuting members of $S^\perp$. From here it follows that, if Γ has rank $n - t$, then $S^\perp$ comprises 2^t copies of a group that is isomorphic to $\tilde{S}^\perp$, where $\tilde{S}^\perp$ is generated from the rows of $\tilde{\mathcal{A}}^\perp$, where $\tilde{\mathcal{A}}^\perp$ is obtained from $\mathcal{A}^\perp$ by deleting t dependent rows and corresponding columns of $\mathcal{A}^\perp$. We then consider the maximum commuting subgroups of $\tilde{S}^\perp$ instead of $S^\perp$. Equivalently we reduce Γ to $\tilde{\Gamma}$, being a $n - t \times n - t$ matrix of maximum rank, and look for two vectors $v, v' \in \mathbb{F}_2^{n-t}$ that satisfy $v\tilde{\Gamma}v'^T = 0$. More generally, by linearity, there exist size 2^h subgroups of F_2^{n-t} (linear subspaces), L_B, as generated by $h \times n$ binary matrices, B, that satisfy $B\tilde{\Gamma}B^T = 0$. Each such linear subspace, L_B, defines a commuting subgroup of $\tilde{S}^\perp$.

Lemma 10 *Let Γ have rank $n - t$, and let $\tilde{\Gamma}$ be a $n - t \times n - t$ maximum rank matrix obtained from Γ by removing t linearly dependent rows and corresponding columns. There are multiple choices for $\tilde{\Gamma}$. Then each commuting subgroup, $\tilde{P}$ of $\tilde{S}^\perp$, as described by some B satisfying $B\tilde{\Gamma}B^T = 0$, is in one-to-one correspondence with a commuting subgroup, P, of $S^\perp$, as described by some $\hat{B}$ satisfying $\hat{B}\Gamma\hat{B}^T = 0$, where $|P| = 2^t|\tilde{P}|$.*

Proof. Let Q be a set of t linearly dependent rows of Γ. For some $u, u' \in \mathbb{F}_2^n$ let $u\Gamma u'^T = 0$. Then $u, u' \in L_{\hat{B}}$ for some $\hat{B}$. Then $\exists w, w'$, uniquely, such that $u\Gamma = w\Gamma$ and $u'\Gamma = w'\Gamma$, where w and w' are both zero at all positions defined by elements in Q. Then we can delete those t rows of Γ, defined by the elements in Q, and the corresponding columns, as Γ is symmetric, and the corresponding elements of w, w' to obtain and work with $\tilde{\Gamma}$ and v, v', where $v, v' \in L_B$. Due to the unique mapping from $u, u' \to w, w' \to v, v'$, the commutative subgroups from $\tilde{\Gamma}$ are in one-to-one correspondence with those from Γ, but 2^t times smaller due to the restriction to 0 for t positions, specified by Q, in u, u'. □

So 2^t copies of a commuting subgroup of $\tilde{S}^\perp$ comprise a commuting subgroup of $S^\perp$. We are particularly interested in the maximum size commuting subgroups of $\tilde{S}^\perp$ and $S^\perp$, i.e. in those subgroups that cannot be contained in larger commuting subgroups. In terms of the binary representation, this translates into finding matrices B where h is maximised, and such that $B\tilde{\Gamma}B^T = 0$. Thus our question simplifies to finding the largest $h \times n - t$ B matrices such that $B\tilde{\Gamma}B^T = 0$. Remember that $e = \frac{\text{rank}(\Gamma)}{2} = \frac{n-t}{2}$.

Theorem 2 *All maximum commuting subgroups of $\tilde{S}^\perp$ and $S^\perp$ are of size 2^e and 2^{n-e}, respectively. Moreover there are $\chi_e = \prod_{j=1}^e (2^j + 1)$ such groups in both cases, and each element is in $\prod_{j=1}^{e-1} (2^j + 1)$ such groups.*

Proof. Let the rows, B_j, of B generate the linear subspace, L. Observe that $\tilde{\Gamma}$ has a zero diagonal. Therefore any $B_j \in F_2^{n-t}$ satisfies $B_j \tilde{\Gamma} B_j^T = 0$, and therefore so does any member of L. The maximum size of L is then derived as follows.

- Choose non-zero $B_0 \in F_2^{n-t}$ such that $B_0 \tilde{\Gamma} B_0^T = 0$. There are $2^{n-t} - 1$ such choices.

- Choose non-zero $B_1 \in F_2^{n-t}$, $B_1 \neq B_0$, such that any member, b, of the linear space generated by $\{B_0, B_1\}$ satisfies $b\tilde{\Gamma}b^T = 0$. There are $2^{n-t} - 2^1$ such choices.

- Choose non-zero $B_2 \in F_2^{n-t}$, B_2 not in the linear space generated by $\{B_0, B_1\}$, such that any member, b, of the linear space generated by $\{B_0, B_1, B_2\}$ satisfies $b\tilde{\Gamma}b^T = 0$. There are $2^{n-t} - 2^2$ such choices.

- ... and so on.

We continue in this manner until there are no more choices. Thus B always has a maximum of e rows, i.e. a maximum commuting subgroup of $\tilde{S}^\perp$ is always size 2^e. In total we generate $\prod_{j=0}^{e-1}(2^{n-t-j} - 2^j)$ linear subspaces. But, for M a maximum rank $e \times e$ binary matrix, $B' = MB$ generates the same linear subspace as B. We have to remove such repetitions. M is chosen from $\mathrm{GL}(e, 2)$ and $|\mathrm{GL}(e,2)| = \prod_{j=0}^{e-1}(2^e - 2^j)$, so the total number of unique linear subspaces, i.e. of maximum commuting subgroups of $\tilde{S}^\perp$, is $\chi_e = \frac{\prod_{j=0}^{e-1}(2^{n-t-j}-2^j)}{\prod_{j=0}^{e-1}(2^e-2^j)} = \prod_{j=1}^{e}(2^j + 1)$. For $S^\perp$ we simply multiply the maximum commutative subgroup size of $\tilde{S}^\perp$ by 2^t, as there are t redundant rows/columns, to get $2^{n-e} = 2^e \times 2^t$. The number of maximum commutative subgroups remains at $\chi_e = \prod_{j=1}^{e}(2^j + 1)$.

Each element is in $\prod_{j=1}^{e-1}(2^{n-t-j} - 2^j)$ linear subspaces, since we fix the first element. There are $\prod_{j=1}^{e-1}(2^e - 2^j)$ repetitions (the elements in $\mathrm{GL}(e, 2)$ with fixed first row), so each element is in $\frac{\prod_{j=1}^{e-1}(2^{n-t-j}-2^j)}{\prod_{j=1}^{e-1}(2^e-2^j)} = \prod_{j=1}^{e-1}(2^j + 1)$ such groups. $\square$

It is interesting to note that χ_e is also the total number of binary self-dual codes of length $2(e+1)$. This leads us to make a passing observation regarding the multiplicative order of $\tilde{\Gamma}$.

Lemma 11 *Let u be the multiplicative order of $\tilde{\Gamma}$, i.e. let $\tilde{\Gamma}^u = I$ for some minimum positive u. Then u is even and $\tilde{\Gamma}$ cannot be factored as $\tilde{\Gamma} = \Omega\Omega^T$ for some Ω.*

Proof. If u is odd or if $\exists \Omega$ such that $\tilde{\Gamma} = \Omega\Omega^T$ then we show that $\exists B$ matrices of size $\frac{n-t}{2} \times n - t$ such that $B\tilde{\Gamma}B^T = 0$, where the set of B matrices is in one-to-one correspondence with the set of self-dual binary codes of length $2e$ and dimension e, implying that there are χ_{e-1} of them. But this is impossible as, by theorem 2, there are χ_e of them. The argument is as follows. If u is odd then $B\tilde{\Gamma}B^T = C\tilde{\Gamma}^{\frac{u-1}{2}}\tilde{\Gamma}\tilde{\Gamma}^{\frac{u-1}{2}}C^T = CC^T = 0$, where $B = C\tilde{\Gamma}^{\frac{u-1}{2}}$. If $\tilde{\Gamma} = \Omega\Omega^T$ then $B\tilde{\Gamma}B^T = CC^T = 0$, where $C = B\Omega$. In both cases C is taken from the set of matrices that generate self-dual binary codes of length $n - t$ and dimension $\frac{n-t}{2}$, where $B = C\tilde{\Gamma}^{\frac{u-1}{2}}$ in the first case and $B = C\Omega^{-1}$ in the second case. There are χ_{e-1} such matrices, which contradicts theorem 2. $\square$

Example 4 *Let G be the graph defining a mixed graph state, ρ, stabilised by the rows of*

$$\mathcal{A} = \begin{pmatrix} X \otimes Z \otimes Z \otimes Z \\ I \otimes X \otimes I \otimes I \\ I \otimes Z \otimes X \otimes Z, \\ I \otimes I \otimes Z \otimes X \end{pmatrix}.$$ *We want to find all maximal commutative subgroups of $S^\perp$. The*

adjacency matrix of G_b is $\Gamma = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$, *which has full rank, so $\tilde{\Gamma} = \Gamma$. Therefore*

$t = 0$, $e = \frac{rank(\Gamma)}{2} = \frac{n-t}{2} = 2$, and the size of a maximal commutative subgroup of $S^\perp$ is $2^{n-e} = 2^2 = 4$. Moreover, $\Gamma^u = \Gamma^4 = I$.

From theorem 2 there are $\chi_e = 15$ maximum commuting subgroups of $S^\perp$ and these can be generated by 15 matrices, B, satisfying $B\tilde{\Gamma}B^T = 0$, where the B can be chosen, (non-uniquely) from

$$\begin{pmatrix} 1000 \\ 0110 \\ 0100 \\ 1011 \\ 1010 \\ 1001 \end{pmatrix}, \begin{pmatrix} 1000 \\ 0101 \\ 1100 \\ 0010 \\ 1010 \\ 1101 \end{pmatrix}, \begin{pmatrix} 1000 \\ 0011 \\ 1100 \\ 1001 \\ 0110 \\ 0001 \end{pmatrix}, \begin{pmatrix} 0100 \\ 1010 \\ 0010 \\ 0001 \\ 0110 \\ 1001 \end{pmatrix}, \begin{pmatrix} 0100 \\ 0001 \\ 0010 \\ 1101 \\ 1011 \\ 0111 \end{pmatrix}.$$

For instance, $B = \begin{pmatrix} 1100 \\ 1001 \end{pmatrix}$ acting multiplicatively on the rows of $\mathcal{A}^T$ generates the maximum commuting subgroup with elements $\{I \otimes I \otimes I \otimes I, \quad \mp iY \otimes X \otimes Z \otimes I, \quad \mp iY \otimes I \otimes Z \otimes X, \quad I \otimes X \otimes I \otimes X\}$. Similarly, $B = \begin{pmatrix} 1011 \\ 0111 \end{pmatrix}$ acting multiplicatively on the rows of $\mathcal{A}^T$ generates the maximum commuting subgroup with elements $\{I \otimes I \otimes I \otimes I, \quad \mp iX \otimes I \otimes Y \otimes Y, \quad \mp iZ \otimes X \otimes X \otimes Y, \quad \mp iY \otimes X \otimes Z \otimes I\}$. Observe that, in this case, $\mp iY \otimes X \otimes Z \otimes I$ occurs in both subgroups. More generally, each group element occurs in 3 maximal commutative subgroups.

Example 5 *Let G be the graph defining a mixed graph state, ρ, stabilised by the rows of*

$$\mathcal{A} = \begin{pmatrix} X \otimes Z \otimes I \\ I \otimes X \otimes Z \\ Z \otimes I \otimes X \end{pmatrix}.$$ *The adjacency matrix of G_b is* $\Gamma = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$, *which has rank 2. Therefore $t = 1$, and $e = \frac{n-t}{2} = 1$, and the size of a maximal commutative subgroup of $S^\perp$ is $2^{n-e} = 2^2 = 4$. By removing one dependent row and corresponding column of Γ (we choose the last row/column) we can obtain a $\tilde{\Gamma} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.*

From theorem 2 there are $\chi_e = 3$ maximum commuting subgroups of $S^\perp$ and these can be generated by extensions of 3 matrices, B, satisfying $B\tilde{\Gamma}B^T = 0$, where the B are

$$(\; 10 \;), \quad (\; 01 \;), \quad (\; 11 \;).$$

Noting that the last row/column of Γ is dependent because $\Gamma_0 + \Gamma_1 + \Gamma_2 = 000$, we obtain the three maximum commuting subgroups of $S^\perp$ via the 3 matrices, B', these being

$$\begin{pmatrix} 100 \\ 111 \end{pmatrix}, \quad \begin{pmatrix} 010 \\ 111 \end{pmatrix}, \quad \begin{pmatrix} 110 \\ 111 \end{pmatrix},$$

leading to the following three maximum commuting subgroups of $S^\perp$, respectively: $\{I \otimes I \otimes I, X \otimes I \otimes Z, \mp iY \otimes IY \otimes Y, \mp iZ \otimes Y \otimes X\}$, $\{I \otimes I \otimes I, Z \otimes X \otimes I, \mp iY \otimes IY \otimes Y, \pm iX \otimes Z \otimes Y\}$, $\{I \otimes I \otimes I, \mp Y \otimes X \otimes Z, \mp iY \otimes IY \otimes Y, I \otimes Z \otimes X\}$.

Lemma 12 *Let G and H be two mixed graphs on n variables. If they have the same mixed rank e, there exists an isomorphism between their commutative subgroups.*

Proof. Assume first $n = 2e$. Then, the linear group generated by their respective Γ is in both cases $\mathbb{F}_2^e$. The isomorphism is given by sending the basis elements of $\langle \Gamma^G \rangle$ (i.e., the rows of Γ^G) to the corresponding elements in $\langle \Gamma^H \rangle$. Their commutative properties are the same, so this isomorphism preserves commutatitivity.

For $n > 2e$, the linearly dependent elements can be expressed as $\Gamma_j^G = \sum_K \Gamma_k^G$, and similarly (after a possible reordering, that is, a permutation of the nodes) $\Gamma_j^H = \sum_{K'} \Gamma_k^H$. The isomorphism for the independent rows is the same as before. For the dependent rows, we send $\mathcal{A}_j^T \mathcal{A}_K^T$ to $\mathcal{A}_j^T \mathcal{A}_{K'}^T$. This sends the row $00 \ldots 0$ to itself, and commutativity is preserved by linearity. $\square$

Example 6 *Let G_b be the line in 4 variables, with adjacency matrix $\Gamma = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$, and the complete graph in 4 variables. Both of them have $e = 2$. The group generated by the respective adjacency matrices is $\mathbb{F}_2^4$. We have the isomorphism $f : S_{Line}^T \to S_{Complete\ graph}^T$ defined by $f(\mathcal{A}_0^T) = \mathcal{A}_{\{0,2,3\}}^T$, $f(\mathcal{A}_1^T) = \mathcal{A}_{\{0,2\}}^T$, $f(\mathcal{A}_2^T) = \mathcal{A}_{\{1,3\}}^T$, $f(\mathcal{A}_3^T) = \mathcal{A}_{\{0,1,3\}}^T$. In particular, the commutative subgroup on the line generated by $\mathcal{A}_0^T, \mathcal{A}_3^T$ corresponds to the commutative subgroup on the complete graph generated by $\mathcal{A}_{\{0,2,3\}}^T, \mathcal{A}_{\{0,1,3\}}^T$.*

Example 7 *let G be the triangle on 3 variables, and H the star graph on 3 variables. For both of them, $e = 1$. A possible isomorphism is given by $f : S_G^T \to S_H^T$, defined by $f(\mathcal{A}_0^T) = \mathcal{A}_0^T$, $f(\mathcal{A}_1^T) = \mathcal{A}_1^T$, $f(\mathcal{A}_2^T) = \mathcal{A}_{\{0,2\}}^T$. In particular, the commutative subgroup on G generated by $\mathcal{A}_1^T, \mathcal{A}_{\{0,2\}}^T$ corresponds to the commutative subgroup on H generated by $\mathcal{A}_1^T, \mathcal{A}_2^T$. Note that if we take the isomorphism given by $f : S_G^T \to S_H^T$, defined by $f(\mathcal{A}_0^T) = \mathcal{A}_0^T$, $f(\mathcal{A}_1^T) = \mathcal{A}_2^T$, $f(\mathcal{A}_2^T) = \mathcal{A}_{\{0,1\}}^T$, we obtain the same commutative subgroups.*

5 Children of pure graph state parents

In this section, given a binary string of length n, $j = j_0 \cdots j_{n-1}$, we define $\overleftarrow{s}_j := \mathcal{A}_K^T$, where $K = \{i : j_i = 1\}$, where $\overleftarrow{s}_{0\ldots00} = I$. Remember that, for $i, i' \in K$, $i' > i$, we define $\mathcal{A}_K^T$ to

contain the multiplicative factor $\mathcal{A}_i^T \mathcal{A}_{i'}^T$. However the ordering $\mathcal{A}_i^T \mathcal{A}_{i'}^T$ is just as valid and differs by a global multiplicative factor of -1 if $\mathcal{A}_i^T$ and $\mathcal{A}_{i'}^T$ anti-commute. This situation carries over to the $\overleftarrow{s}_j$. In theorem 3, and for such cases where $\overleftarrow{s}_j$ contains anti-commuting factors, the b_j are therefore only defined up to ± 1. Let $L_m = \{v : (\mathcal{A}^e)_{v,n+m} = Z$ or $Y\}$, and let $J = \{x \in \mathbb{F}_2^n \mid \mathcal{I}(x) = 1\}$, where $\mathcal{I}(x) = \prod_{m=0}^{e-1}(1 + \sum_{k \in L_m} x_k) = \prod_{m=0}^{e-1} \mathcal{I}_m(x)$.

Theorem 3 *Given a child, ρ, of a pure graph state parent of a mixed graph, corresponding to a symmetric extension of $\mathcal{A}$ by e columns and rows, $\mathcal{A}^e$, we can write ρ as:*

$$\rho = \frac{1}{2^n} \sum_{j \in J} b_j \overleftarrow{s}_j, \qquad b_j \in \{\pm 1, \pm i\}, \forall j,$$

where all $\overleftarrow{s}_j$, $j \in J$, commute pairwise, and if $\overleftarrow{s}_j, \overleftarrow{s}_{j'}$ are present in the sum, so is $\overleftarrow{s}_j \overleftarrow{s}_{j'} = \overleftarrow{s}_{j+j'}$, implying that $\{\overleftarrow{s}_j : j \in J\}$ is a commutative subgroup of $S^\perp$.

Let $j^\alpha \in \mathbb{F}_2^n$ and $j^{\alpha,\beta} \in \mathbb{F}_2^n$, $0 \le \alpha, \beta < n$ be weight-one and weight-two binary vectors with 1's only in positions α, and α and β, respectively.

Lemma 13 *Given a child, ρ, of a pure graph state parent of a mixed graph, described by $\mathcal{A}^e$, the coefficients, b_j, in the sum of theorem 3, are as follows:*

- *Case $e = 1$:*

    - *If $\overleftarrow{s}_{j^\alpha}$ is present in the sum then $b_{j_\alpha} = +1$.*
    - *If $\overleftarrow{s}_{j^{\alpha,\beta}}$ is present in the sum then we have two cases:*
        1. *if $\overleftarrow{s}_{j^\alpha}$ and $\overleftarrow{s}_{j^\beta}$ anticommute, then $\exists\, a, b \in \{\alpha, \beta\}$ such that $(\mathcal{A}^e)_{a,n} = Z$ and $(\mathcal{A}^e)_{b,n} = Y$; furthermore, the corresponding term in the sum will be equal to $\pm i \mathcal{A}_{\{\alpha,\beta\}}^T = i\mathcal{A}_a^T \mathcal{A}_b^T$, so $b_{j^{\alpha,\beta}} = \pm i$.*
        2. *if $\mathcal{A}_\alpha^T$ and $\mathcal{A}_\beta^T$ commute, the corresponding term in the sum will be equal to $\mathcal{A}_{\{\alpha,\beta\}}^T$, and $b_{j^{\alpha,\beta}} = 1$.*
    - *Any other matrices, $\mathcal{A}_K^T$, will be products of $\mathcal{A}_{K_j}^T$ also present in the sum, with K_j of size 1 and size 2. Furthermore, their coefficients are given by the multiplication of the coefficients of the terms into which it is decomposed.*

- *General e: The coefficient of $\mathcal{A}_K^T$, with K of size 1 or 2 is given by the multiplication together of the coefficients, one from each extension column. In this case, there might be nondecomposable terms. However, the coefficient of a term will be giving by multiplying the coefficients obtained by taking each column separately.*

- *Furthermore, for any e, if we change the sign of a term $\mathcal{A}_k^T$, $0 \le k < n$, then we add the Boolean linear term x_k to the quadratic Boolean representation of the pure parent graph state, or if we change the sign of $\mathcal{A}_K^T$, for K a set of size $t > 1$ present in the sum, we add any of the Boolean linear terms x_k for each k s.t. $(\mathcal{A}^e)_{n+j,k} = Y$ or $(\mathcal{A}^e)_{n+j,k} = Z$.*

Example 8 *Let the directed triangle be defined by the stabilizer basis $\mathcal{A}_0 = X \otimes Z \otimes I$, $\mathcal{A}_1 = I \otimes X \otimes Z$, $\mathcal{A}_2 = Z \otimes I \otimes X$. Then the basis of $S^\perp$ is given by reversing the arrows: $\mathcal{A}_0^T = X \otimes I \otimes Z$, $\mathcal{A}_1^T = Z \otimes X \otimes I$, $\mathcal{A}_2^T = I \otimes Z \otimes X$, so $S^\perp = \{\overleftarrow{s}_{000} = I \otimes I \otimes I, \overleftarrow{s}_{100} = X \otimes I \otimes Z, \overleftarrow{s}_{010} = Z \otimes X \otimes I, \overleftarrow{s}_{110} = -iY \otimes X \otimes Z, \overleftarrow{s}_{001} = I \otimes Z \otimes X, \overleftarrow{s}_{101} = iX \otimes Z \otimes Y, \overleftarrow{s}_{011} = -iZ \otimes Y \otimes X, \overleftarrow{s}_{111} = -iY \otimes Y \otimes Y\}$.*

One of the two parents is formed by adding the column $(X\ Z\ Y)^T$ to $\mathcal{A}$, giving the parent $i^{2(x_0 x_2 + x_1 x_2 + x_1 x_3 + x_2 x_3 + x_2) + x_2} = i^{2(x_0 x_2 + x_1 x_2 + x_2 + (\mathcal{I}(x)+1)x_3) + x_2}$. Here $L_3 = \{1, 2\}$, and $\mathcal{I}(x) = x_1 + x_2 + 1$, so $J = \langle 100, 011 \rangle = \{000, 100, 011, 111\}$. We can re-interpret $\mathcal{I}(x)$ and J as parity and generator matrices, H and G, respectively, where $H = \begin{pmatrix} 011 \end{pmatrix}$ and $G = \begin{pmatrix} 100 \\ 011 \end{pmatrix}$, and where G generates the binary linear code with codewords in set J. By tracing over the environmental qubit, x_3, we get

$$\rho = \frac{1}{8}\left(I \otimes I \otimes I + X \otimes I \otimes Z + Z \otimes Y \otimes X + Y \otimes Y \otimes Y\right) = \frac{1}{8}\left(\overleftarrow{s}_{000} + \overleftarrow{s}_{100} + i\overleftarrow{s}_{011} + i\overleftarrow{s}_{111}\right).$$

Note that $X \otimes I \otimes Z$ and $Z \otimes Y \otimes X$ commute, and that $(X \otimes I \otimes Z) \cdot (Z \otimes Y \otimes X) = Y \otimes Y \otimes Y$. We can obtain another parent for the same child by doing a local complementation (LC) on vertex 3 (i.e. LC_3) on the graph described by the parent. This is an LC in the environment. If one describes the $\mathbb{Z}_4$-linear offsets of the parent by black vertices in the graph, then LC_3 swaps the vertex neighbours of vertex 3 from black $\leftrightarrow$ white.

The other of the two parents is formed by adding the column $(X\ Y\ Z)^T$ to $\mathcal{A}$, giving the parent $i^{2(x_0 x_2 + x_1 + x_1 x_3 + x_2 x_3) + x_1} = i^{2(x_0 x_2 + x_1 + (\mathcal{I}(x)+1)x_3) + x_1}$. Once again $L_3 = \{1, 2\}$, $\mathcal{I}(x) = x_1 + x_2 + 1$, and $J = \{000, 100, 011, 111\}$. By tracing over the environmental qubit, x_3, we get

$$\rho = \frac{1}{8}\left(I \otimes I \otimes I + X \otimes I \otimes Z - Z \otimes Y \otimes X - Y \otimes Y \otimes Y\right) = \frac{1}{8}\left(\overleftarrow{s}_{000} + \overleftarrow{s}_{100} - i\overleftarrow{s}_{011} - i\overleftarrow{s}_{111}\right).$$

H and G are unchanged. Observe that the second parent is obtained from the first by swapping the positions of Y and Z in rows 1 and 2 of the extra column (column 3). In terms of the Boolean function representation of the parents, this translates to adding the Boolean quadratic term $x_1 x_2 + x_1 + x_2$, and removing x_2 and adding x_1 $\mathbb{Z}_4$-linear terms. Observe that the coefficients of the Pauli basis terms $Z \otimes Y \otimes X$ and $Y \otimes Y \otimes Y$ are multiplied by -1. This is because both terms are generated from rows 1 and 2 of $\mathcal{A}^T$ which are the rows where Y and Z are swapped in $\mathcal{A}^e$.

For each parent we can also consider how the addition of binary linear terms (in the lab) affects the resultant child density matrix. We don't currently consider the addition of binary linear terms in the environment (i.e. x_3 for this example). For instance, for the addition of column $(X\ Z\ Y)^T$ then $i^{2(x_0 x_2 + x_1 x_2 + x_1 x_3 + x_2 x_3 + x_0 + x_2) + x_2}$, i.e. the addition of x_0, simply flips the signs of $X \otimes I \otimes Z$ and $Y \otimes Y \otimes Y$ as both terms have row 0 of $\mathcal{A}^T$ as a factor. However addition of x_1 or x_2 has the same effect as swapping Y and Z in rows 1 and 2, so swaps between the two parents. Thus the addition of $\bar{\mathcal{I}}(x) = \mathcal{I}(x) + 1$ fixes the child density matrix. So we have the following maps for $a \in \{0, 1\}$:

child $= 8\rho$	parent
$I \otimes I \otimes I + X \otimes I \otimes Z + Z \otimes Y \otimes X + Y \otimes Y \otimes Y$	$2(x_0x_2 + x_1x_2 + x_2 + \bar{\mathcal{I}}(x)(x_3 + a)) + x_2,$
	$2(x_0x_2 + x_1 + x_2 + \bar{\mathcal{I}}(x)(x_3 + a)) + x_1,$
$I \otimes I \otimes I - X \otimes I \otimes Z + Z \otimes Y \otimes X - Y \otimes Y \otimes Y$	$2(x_0x_2 + x_1x_2 + x_0 + x_2 + \bar{\mathcal{I}}(x)(x_3 + a)) + x_2,$
	$2(x_0x_2 + x_0 + x_1 + x_2 + \bar{\mathcal{I}}(x)(x_3 + a)) + x_1,$
$I \otimes I \otimes I + X \otimes I \otimes Z - Z \otimes Y \otimes X - Y \otimes Y \otimes Y$	$2(x_0x_2 + x_1 + \bar{\mathcal{I}}(x)(x_3 + a)) + x_1,$
	$2(x_0x_2 + x_1x_2 + x_1 + x_2 + \bar{\mathcal{I}}(x)(x_3 + a)) + x_2,$
$I \otimes I \otimes I - X \otimes I \otimes Z - Z \otimes Y \otimes X + Y \otimes Y \otimes Y$	$2(x_0x_2 + x_0 + x_1 + \bar{\mathcal{I}}(x)(x_3 + a)) + x_1,$
	$2(x_0x_2 + x_1x_2 + x_0 + x_1 + x_2 + \bar{\mathcal{I}}(x)(x_3 + a)) + x_2.$

Other children given by the extensions $(Z \ X \ Y)^T$ *and* $(Z \ Y \ X)^T$ *are respectively*

$$\rho_1 = \tfrac{1}{8}\left(I \otimes I \otimes I + aZ \otimes X \otimes I + bX \otimes Z \otimes Y + cY \otimes Y \otimes Y\right) = \tfrac{1}{8}\left(\overleftarrow{s}_{000} + a\overleftarrow{s}_{010} - bi\overleftarrow{s}_{101} + ci\overleftarrow{s}_{111}\right)$$

$$\rho_2 = \tfrac{1}{8}\left(I \otimes I \otimes I + aY \otimes X \otimes Z + bI \otimes Z \otimes X + cY \otimes Y \otimes Y\right) = \tfrac{1}{8}\left(\overleftarrow{s}_{000} + ai\overleftarrow{s}_{110} + b\overleftarrow{s}_{001} + ci\overleftarrow{s}_{111}\right)$$

with condition $c = ab,$ $a, b \in \{1, -1\}$ *in both cases.*

Example 9 *Let a mixed 6-clique graph be defined by the stabilizer basis* $\mathcal{A} = \begin{pmatrix} X & Z & Z & Z & Z & Z \\ I & X & Z & Z & Z & Z \\ I & I & X & Z & Z & Z \\ I & I & I & X & Z & Z \\ I & I & I & I & X & Z \\ I & I & I & I & I & X. \end{pmatrix}$.

Then the basis of $S^\perp$ *is obtained from* $\mathcal{A}^T$. *The parents are obtained by adding* $e = 3$ *columns to* $\mathcal{A}$, *with subsequent addition of* $e = 3$ *rows. For instance, one parent is given by*

$$\mathcal{A}^e = \begin{pmatrix} X & Z & Z & Z & Z & Z & X & I & X \\ I & Y & Z & Z & Z & Z & Y & I & X \\ I & I & X & Z & Z & Z & Z & I & X \\ I & I & I & X & Z & Z & I & X & Y \\ I & I & I & I & X & Z & I & Y & Y \\ I & I & I & I & I & X & I & Z & Y \\ I & Z & Z & I & I & I & X & I & I \\ I & I & I & I & Z & Z & I & X & I \\ I & I & I & Z & Z & Z & I & I & X \end{pmatrix} \equiv \begin{pmatrix} X & I & I & I & I & I & I & I & I \\ I & Y & I & I & I & I & Z & I & I \\ I & I & X & I & I & I & Z & I & I \\ I & I & I & Y & Z & Z & I & I & Z \\ I & I & I & Z & X & Z & I & Z & Z \\ I & I & I & Z & Z & Y & I & Z & Z \\ I & Z & Z & I & I & I & X & I & I \\ I & I & I & I & Z & Z & I & X & I \\ I & I & I & Z & Z & Z & I & I & X. \end{pmatrix},$$

which represents $i^{2(x_1x_6 + x_2x_6 + x_3x_4 + x_3x_5 + x_3x_8 + x_4x_5 + x_4x_7 + x_4x_8 + x_5x_7 + x_5x_8 + x_1 + x_3 + x_4 + x_5) + x_1 + x_3 + x_5}$. *Here*
$L_3 = \{1, 2\}$, $L_4 = \{4, 5\}$, *and* $L_5 = \{3, 4, 5\}$, *and* $\mathcal{I}(x) = (x_1 + x_2 + 1)(x_4 + x_5 + 1)(x_3 + x_4 + x_5 + 1)$, *so* $J = < 100000, 011000, 000011 > = \{000000, 100000, 011000, 111000, 000011, 100011, 011011, 111011\}$.
We can re-interpret $\mathcal{I}(x)$ *and* J *as parity and generator matrices,* H *and* G, *respectively,*

where $H = \begin{pmatrix} 011000 \\ 000011 \\ 000111 \end{pmatrix}$ *and* $G = \begin{pmatrix} 100000 \\ 011000 \\ 000011 \end{pmatrix}$, *and where* G *generates the binary linear*

code with codewords in set J. By tracing over the environmental qubits, x_6, x_7, x_8, we get

$$\begin{aligned}
\rho = \ & (I \otimes I \otimes I \otimes I \otimes I \otimes I + X \otimes Z \otimes Z \otimes Z \otimes Z \otimes Z - I \otimes X \otimes Y \otimes I \otimes I \otimes I \\
& -X \otimes Y \otimes X \otimes Z \otimes Z \otimes Z - I \otimes I \otimes I \otimes I \otimes X \otimes Y - X \otimes Z \otimes Z \otimes Z \otimes Y \otimes X \\
& +I \otimes X \otimes Y \otimes I \otimes X \otimes Y + X \otimes Y \otimes X \otimes Z \otimes Y \otimes X).
\end{aligned}$$

Proof. (Theorem 3): The qubits present in each L_m will be the ones connected with the environmental qubit $n + m$, implying that the difference between the measurement in $x_{n+m} = 0$ and $x_{n+m} = 1$ will be the Boolean function $\sum_{k \in L_m} x_k$. The support of ρ will be equal to the binary vectors such that these Boolean functions are 0 for all m. By lemma 1, ρ can be expressed as the sum of some of the matrices on $S^\perp$; by lemma 6, all the matrices in $S^\perp$ have nonintersecting support: ρ will be equal to the sum of the matrices in $S^\perp$ whose support intersects the support of ρ; therefore, it is sufficient to find the nonzero entries of the first row of the matrix. It is easy to check that any matrix in $S^\perp$ has only one nonzero entry on the first row. In other words, ρ will be equal to the sum of the matrices whose support intersects $\{(0, k), k \in K\}$, where $K = \{\sum_{m=0}^{n-1} 2^m b_m, \forall b = b_0 b_1 \ldots b_{n-1} \in J\}$, and J is the indicator of the Boolean function $\prod_{m=0}^{e-1} (\sum_{k \in L_m} x_k + 1)$. To prove that these matrices are the $\overleftarrow{s}_j$, where $j \in J$, we need the following lemma:

Lemma 14 *Let $\overleftarrow{s}_j \in S^\perp$. Then, $(\overleftarrow{s}_j)_{0,t} = 1 \Leftrightarrow k = \sum_{m=0}^{n-1} 2^m j_m$, for $j = j_0 j_1 \ldots j_{n-1}$.*

Proof. Let $\overleftarrow{s}_j = \bigotimes_{R_X} X \bigotimes_{R_Y} Y \bigotimes_{R_Z} Z \bigotimes_{R_I} I$. Let M be a $t \times t$ matrix. Then,

$$M \otimes I = \begin{pmatrix} M & 0 \\ 0 & M \end{pmatrix} \text{ and } M \otimes X = \begin{pmatrix} 0 & M \\ M & 0 \end{pmatrix}$$

Note that X has the same support as Y, and Z has the same support as I, so we only have to consider this two cases. This implies that support$(M \otimes I) =$ support(M), while $(0, k + 2^{t-1}) \in$ support$(M \otimes X) \Leftrightarrow (0, k) \in$ support(M). This implies that $(0, k) \in$ support$(\overleftarrow{s}_j) \Leftrightarrow k = \sum_{m \in R_X \cup R_Y}^{n-1} 2^m m = \sum_{m=0}^{n-1} 2^m j_m$, for $j = j_0 j_1 \ldots j_{n-1}$.
□

To complete the proof of theorem 3, there remains to prove that all $\overleftarrow{s}_j$, $j \in J$ commute pairwise, and if $\overleftarrow{s}_j, \overleftarrow{s}_k$ are present in the sum, so is $\overleftarrow{s}_j \overleftarrow{s}_k$:

First, we shall prove that if $\overleftarrow{s}_j, \overleftarrow{s}_k$ are present in the sum, so is $\overleftarrow{s}_j \overleftarrow{s}_k$: this follows from the indicator J being a linear space, since $\overleftarrow{s}_j \overleftarrow{s}_k$ corresponds to the sum of the Boolean vectors.

Now we shall see that it is commutative: Let $j, k \in J$: We can write $\overleftarrow{s}_j = \prod_{a \in A} \mathcal{A}_a^T$, and $\overleftarrow{s}_k = \prod_{b \in B} \mathcal{A}_b^T$, where $\mathcal{A}_a^T, \mathcal{A}_b^T$ are in the basis of $S^\perp$. Then, the corresponding $\mathcal{A}_a \in S, a \in A$, have an even number of Y and Z in each extension column, and similarly for B. Therefore, both $\overleftarrow{s}_j$ and $\overleftarrow{s}_k$ have either X or I in all extension columns, and therefore they commute.
□

Proof. [Lemma 13] Since all the parent Boolean functions have no constant terms and no linear terms involving the environmental qubits, the first entry in a truth table for each measurement $|\psi_m\rangle$ will always be $+1$. The first row of the density matrix for each measurement

$|\psi_m\rangle$ will therefore be equal to $\frac{1}{2^{n/2}}\langle\psi_m|$. Also, note that the final ρ will be nonzero only where the entries for all $|\psi_m\rangle$ are equal, and will then be equal to any of them; it is therefore enough to look at $\langle\psi_{0\ldots0}|$.

    Case $e = 1$:

- Size 1: By the proof of theorem 3, any term, $\pm\frac{1}{2^n}\mathcal{A}_j^T$, $0 \le j \le n-1$ is such that $(\mathcal{A}^e)_{j,n} = X$ or I. Since row j of the stabilizer of the parent graph state, $\mathcal{A}^e$, is equal to $\mathcal{A}\otimes$(extension entries), there is no linear term x_j in the parent graph, so that the entry $0\ldots1\ldots0$, where the 1 occurs in position u, of $|\psi_{0\ldots0}\rangle$, and therefore of $\langle\psi_{0\ldots0}|$ of the parent is $+\frac{1}{2^{n/2}}$. As the first row of $\mathcal{A}_j^T$ has $+\frac{1}{2^{n/2}}$ in the same position, the coefficient of $\overleftarrow{s}_j$ is $+\frac{1}{2^n}$.

- Size 2: Suppose that the matrix $\mathcal{A}_{\{j,k\}}^T$ $0 \le j,k \le n-1$, is present in the sum. Then:

  - if $\mathcal{A}_j^T$ and $\mathcal{A}_k^T$ anti-commute, the term in the sum will be $\pm\frac{i}{2^n}\mathcal{A}_{\{j,k\}}^T$ $0 \le j,k \le n-1$, since otherwise $\pm\frac{i}{2^n}\mathcal{A}_j^T\mathcal{A}_k^T$ $0 \le j,k \le n-1$ would not be Hermitian. Furthermore, neither $\mathcal{A}_j^T$ or $\mathcal{A}_j^T$ are present in the sum, because by theorem 3 this would imply that both would be present and would therefore be commuting. This implies that $\exists\, a,b \in \{j,k\}$ such that $(\mathcal{A}^e)_{a,n} = Y$ and $(\mathcal{A}^e)_{b,n} = Z$. The first row of $\pm\frac{i}{2^n}\mathcal{A}_j^T\mathcal{A}_k^T$ has its only nonzero entry where $x_j = x_k = 1, x_u = 0\ \forall u \ne j,k$. Therefore, the entry in $|\psi_0\rangle$ will be given by the presence or absence of x_jx_k, x_j, x_k, in the ANF of the parent graph. Since $\mathcal{A}_j^T$ and $\mathcal{A}_k^T$ anti-commute, the restriction of $\mathcal{A}_j, \mathcal{A}_k$ (that also anti-commute) to the pair j,k will give $X_\alpha Z_\beta$ and $I_\alpha X_\beta$ for $\alpha,\beta \in \{j,k\}$. This implies that the restriction of $\mathcal{A}_\alpha^T$ and $\mathcal{A}_\beta^T$ are , respectively, $X_\alpha I_\beta$ and $Z_\alpha X_\beta$, so the restriction of $i\mathcal{A}_\alpha^T\mathcal{A}_\beta^T$ is $Y_\alpha X_\beta$. Note that we only need to look at the restriction, since any further Kronecker product will be by X, Z or I, and these will not change the first non-zero entry.

    * If the extension column gives $(\mathcal{A}^e)_{\alpha,n} = Z$ and $(\mathcal{A}^e)_{\beta,n} = Y$, we get the term $2(x_\alpha x_\beta + x_\beta) + x_\beta$ in the parent graph, so $|\psi_0\rangle$ has entry i for $x_j = x_k = 1, x_u = 0\ \forall u \ne j,k$, which implies that $\langle\psi_0|$ has entry $-i$, same as the same entry in the first row of the matrix given by the order of multiplication $\mathcal{A}_\alpha^T\mathcal{A}_\beta^T$.
    * If the extension column gives $(\mathcal{A}^e)_{\alpha,n} = Y$ and $(\mathcal{A}^e)_{\beta,n} = Z$, we get the term $2x_\alpha + x_\alpha$ in the parent graph, so $|\psi_0\rangle$ has entry $-i$ (so $\langle\psi_0|$ has entry i) for $x_j = x_k = 1, x_u = 0\ \forall u \ne j,k$, same as the same entry in the first row of the matrix given by the order of multiplication $\mathcal{A}_\beta^T\mathcal{A}_\alpha^T$.

  - Suppose $\mathcal{A}_j^T$ and $\mathcal{A}_k^T$ commute. Then, the term $\pm\frac{1}{2^n}\mathcal{A}_j^T\mathcal{A}_k^T$ $0 \le j,k \le n-1$ is present in the sum, the matrices are commuting since $\mathcal{A}_j^T\mathcal{A}_k^T$ is Hermitian. By inspection, on the pair $\mathcal{A}_j, \mathcal{A}_k \in S$, $X_\alpha Z_\beta$ and $Z_\alpha X_\beta$ give entry -1 regardless of extension (note that they have the commuting entry in the extension column), same as $\mathcal{A}_j^T\mathcal{A}_k^T$. As for $X_\alpha I_\beta$ and $I_\alpha X_\beta$ give entry +1 regardless of extension, same as $\mathcal{A}_j^T\mathcal{A}_k^T$.

  - By the proof of theorem 3, $\mathcal{A}_K^T$, $K \subseteq \{0,\ldots,n-1\}$, is present in the sum iff the corresponding stabilizer, $\mathcal{A}_K^T$, has either X or I in the extension column. Therefore,

there exists a (not necessarely unique) decomposition in size 1 and size 2 terms that have either X or I in the extension column (since $YZ = iX$), and, as the entry $x_j = 1 \; \forall j \in A, x_j = 0 \; \forall j \notin A$ will depend on the sum of the terms for the size 1 and size 2 cases, as the Boolean function has degree at most 2, this entry will depend on the entry of the size 1 and size 2 cases, and therefore the coefficient will be the multiplication of the size 1 and size 2 cases (for any given decomposition).

General e: Since the case $e = 1$ was independent of the actual stabilizers (it only depends on the extension), each new column will modify the Boolean expression accordingly. Therefore, the coefficient of any term is given by the multiplication of the coefficient resultant of each extension column.

Change of sign: Let us first assume that j has weight 1, with support in k. Note that each $\mathcal{A}_j^T$ has support in $(0, 2^k)$. In terms of $\langle \psi_{0\ldots0}|$, this means that changing the sign of $\mathcal{A}_j^T$ changes the sign in the jth element in $|\psi_{0\ldots0}\rangle$ (and therefore in $\langle\psi_{0\ldots0}|$). This is equivalent to adding a linear term x_k as long as we change the sign all elements in $|\psi_{0\ldots0}\rangle$ (and therefore in $\langle\psi_{0\ldots0}|$) with $x_k = 1$. Suppose now that j has weight > 1. If we change the sign in j, we have to change also the signs of an odd number of its decomposing terms. Consider therefore the smallest terms present in the group. If the sign changed is of weight 1, see above. If the weight is $t > 1$, with support in $k_1, \ldots, k_t$, then any of the $\mathcal{A}_{k_i}$ are not elements in the subgroup. Adding any linear term x_{k_i} will give the desired matrix, since it is zero in the places were it might differ.

$\square$

Corollary 1 *The commutative subgroup corresponding to a child is maximal.*

Proof. Each column added gives a affine linear Boolean function f_i, which gives a constrain to the indicator J of $f = \prod f_i$. Each constraint, f_i, is nontrivial (that is, not a constant), because if this were the case, then the column would only have X and I, and would therefore be superfluous, yielding a contradiction. The f_i are all independent, otherwise we get redundant columns, yielding a contradiction with e being minimal. Furthermore, any new independent linear constraint reduces by half the size of the indicator, wich means that this size is equal to 2^{n-e}, so it is a maximal commutative subgroup. $\square$

NB: Note that allowing superflous constraints f_i will give *commutative subgroups that are in general not maximal*. In this way, we could also extend graph states in a natural way: the density matrix for the graph state is given by the sum of all the elements of the stabilizer (since it is self-dual), and of course any consistent sign changes that give linear terms (eigenvalue -1). We can however define more density matrices that are stabilized by the stabilizer of the graph state, by allowing also smaller commutative subgroups. For instance, a density matrix associated to the undirected line from 0 to 1 could be then $\rho = a_0 \left(I \otimes I \pm X \otimes Z \pm Z \otimes X \pm Y \otimes Y \right) + a_1 \left(I \otimes I \pm X \otimes Z \right) + a_2 \left(I \otimes I \pm Z \otimes X \right) + a_3 \left(I \otimes I \pm Y \otimes Y \right) + a_4 I \otimes I$, where $\sum a_i = 1$. Note that in the first term, the signs have to be consistent, changing for instance $X \otimes Z$ to $-X \otimes Z$ forces the change $Y \otimes Y$ to $-Y \otimes Y$.

6 Open problem: the weighted sum of a maximal commutative subgroup of $S^\perp$ is a density matrix

Conjecture 1 *Any maximal commutative subgroup corresponds to a child of a pure parent graph, so its weighted sum (with appropiate coefficients) is a density matrix.*

Proof:[incomplete] Let $M^\perp$ be a maximal commutative subgroup of $S^\perp$ for a mixed graph G. Then, the corresponding elements in S commute as well (because direction of arrows is not important), and form a commutative subgroup, M. If there is an extension of S (not unique) to the stabilizer of to a pure graph state, the extension has e columns. Since the elements of M commute, for $e = 1$, we can assign X for all odd products of elements of the basis S, and I to even products. Since it is a subgroup, this is consistent. In general, we can at least always assign either X or I in the corresponding columns of the basis, which respects their commutativity. Not all combinations will be valid (for instance, assigning $I^{\otimes e}$ to a node that does not commute with everybody is not allowed) but there exist at least one such combination, by lemma 18. In general, we still have to prove that this combination is always possible.If it exists, any such combination would have as density matrix the one generated by $M^\perp$.

A possible strategy for finding these extension columns is to write the indicator that will indicate the position of the Y, Z positions. For any nondecomposable $\mathcal{A}_V^T$, we need to impose the condition that in the indicator function, all the x_j, $j \in V$, are equal. This we can achieve by taking the products $\prod(x_j + k_k + 1)$. This strategy works for non-intersecting elements.

Lemma 15 *Regardless of whether we get intersecting elements or not, we always obtain e terms in the final product of the indicator.*

Proof: Let M be a maximal commutative subgroup. By theorem 2, $|M| = 2^{n-e}$. Let C be the corresponding binary linear code. A binary linear code with $k = n - e$ independent codewords has a parity-check matrix with e rows: the product of any set of these e parity-check conditions will be our indicator function.
Note that since $e \leq \frac{n}{2}$ by definition, we have $2e \leq n$, which means that $e \leq n - e$.

Example 10 *Consider the mixed graph given by*

$$
\begin{pmatrix}
X \otimes Z \otimes I \otimes I \otimes Z & = \mathcal{A}_0 \\
I \otimes X \otimes Z \otimes I \otimes Z & = \mathcal{A}_1 \\
I \otimes I \otimes X \otimes Z \otimes Z & = \mathcal{A}_2 \\
I \otimes I \otimes I \otimes X \otimes Z & = \mathcal{A}_3 \\
I \otimes I \otimes I \otimes I \otimes X & = \mathcal{A}_4
\end{pmatrix}
$$

Then, the dual is

$$
\begin{pmatrix}
X \otimes I \otimes I \otimes I \otimes I & = \mathcal{A}_0^T \\
Z \otimes X \otimes I \otimes I \otimes I & = \mathcal{A}_1^T \\
I \otimes Z \otimes X \otimes I \otimes I & = \mathcal{A}_2^T \\
I \otimes I \otimes Z \otimes X \otimes I & = \mathcal{A}_3^T \\
Z \otimes Z \otimes Z \otimes Z \otimes X & = \mathcal{A}_4^T
\end{pmatrix}
$$

The rank of the corresponding adjacency matrix is 4, so $e = 2$. Commuting with $\mathcal{A}_0^T$ is the subgroup generated by $\mathcal{A}_0^T, \mathcal{A}_2^T, \mathcal{A}_3^T, \mathcal{A}_{\{1,4\}}^T = \mathcal{A}_4^T \mathcal{A}_1^T$. But not all of them commute so we choose another element in this subgroup. Commuting (e.g.) with both $\mathcal{A}_0^T$ and $\mathcal{A}_3^T$ is the subgroup generated by $\mathcal{A}_0^T, \mathcal{A}_3^T, \mathcal{A}_{\{1,2,4\}}^T$. This is a maximal commutative subgroup. We shall find an extension of the stabilizers such that we obtain a parent pure graph state.

For any nondecomposable $\mathcal{A}_D^T$, we need to impose the condition that in the indicator function, all the x_j, $j \in D$, are equal. This we can achieve by taking the products $\prod(x_j + k_k + 1)$. Here we have the composite $\mathcal{A}_{\{1,2,4\}}^T$, which gives the condition $(x_1 + x_4 + 1)(x_2 + x_4 + 1)$ (or any of the equivalent conditions). We assign then in the first column of the extension the entries Z, Y to positions $1, 4$, while the remaining entries of the first column will be X or I. Since rows 1 and 4 anti-commute, we assign Z to position 1 and Y to position 4 (note that the other noncommutative choice will give the same commutative subgroup, with a change of sign in $\mathcal{A}_{\{1,2,4\}}^T$). Both $\mathcal{A}_0^T$ and $\mathcal{A}_2^T$ anti-commute with $\mathcal{A}_1^T$ and $\mathcal{A}_4^T$, so we assign X to positions 0 and 2. Finally, we assign I to position 3. Now for the second column: Here we assign Z or Y to positions 2 and 4, while we assign X or I to the remaining nodes. Since $\mathcal{A}_2'^T$ and $\mathcal{A}_4'^T$ commute, we give them the same entry, say Z. Now, $\mathcal{A}_0'^T$ is already commutative with all the other rows, so we assign I to position 0, and I to position 1 for the same reason. We assign X to position 3, since $\mathcal{A}_3'^T$ anti-commutes with both $\mathcal{A}_2'^T$ and $\mathcal{A}_4'^T$. This is now a fully commuting set:

$$\begin{pmatrix} X \otimes Z \otimes I \otimes I \otimes Z & X & I \\ I \otimes X \otimes Z \otimes I \otimes Z & Z & I \\ I \otimes I \otimes X \otimes Z \otimes Z & X & Z \\ I \otimes I \otimes I \otimes X \otimes Z & I & X \\ I \otimes I \otimes I \otimes I \otimes X & Y & Z \end{pmatrix}$$

Example 11 *Let G be the arrrowed 6-clique given by the following stabilizer basis:*

$$\begin{pmatrix} X & Z & Z & Z & Z & Z \\ I & X & Z & Z & Z & Z \\ I & I & X & Z & Z & Z \\ I & I & I & X & Z & Z \\ I & I & I & I & X & Z \\ I & I & I & I & I & X \end{pmatrix}$$

Then, $e = 3$. A maximal commutative subgroup is generated by $\mathcal{A}_0^T, \mathcal{A}_{\{1,2\}}^T, \mathcal{A}_{\{3,4\}}^T$. This gives the indicator $(x_1 + x_2 + 1)(x_3 + x_4 + 1)(x_5 + 1)$. According to this, we assign in the first extension column the entries Z and Y to positions 1 and 2, respectively since their respective rows anti-commute. The remaining entries on this column have to be either X or I. We assign X to positions 0,3,4,5, because their respective rows anti-commute with both. Now for the second column: We assign Z and Y to positions 3 and 4, respectively since their respective rows anti-commute. The remaining entries on this column have to be either X or I. We assign X to positions 0 and 5, because their respective rows (still) anti-commute with both, I to positions 1 and 2, which respective rows now commute with all rows. Finally, in

the last column we assign Z to position 5. The remaining entries on this column have to be either X or I. We assign X to position 0, and I to all the other positions, since their rows all commute pairwise now. This is now a fully commuting set.

$$\begin{pmatrix} X & Z & Z & Z & Z & Z & X & X & X \\ I & X & Z & Z & Z & Z & Z & I & I \\ I & I & X & Z & Z & Z & Y & I & I \\ I & I & I & X & Z & Z & X & Z & I \\ I & I & I & I & X & Z & X & Y & I \\ I & I & I & I & I & X & X & X & Z \end{pmatrix}$$

7   Appendix A

We re-iterate that, as with S, if some or all the rows of $\mathcal{A}$ pairwise anti-commute, then some or all of the members of $S^\perp$ are defined up to a global constant of ± 1. This does not affect the commutation relations between members of S and $S^\perp$. But which members of $S^\perp$ are defined up to ± 1 and how many of them? Consider the n-vertex mixed graph $\overleftrightarrow{G}$ with adjacency matrix A^T, derived from $\mathcal{A}^T$. Then G_b is also the undirected graph associated with $\overleftarrow{G}$ (as well as with G), as G_b has adjacency matrix $\Gamma = A + A^T$. Then the members of $S^\perp$ associated with a $+1$ coefficient are obtained as the subset of row products of $\mathcal{A}^T$ indexed by sets representing all possible independent sets in G_b. But how to compute these sets? For a set w, the *power set* of w, $\mathcal{P}(w)$ is the set of all subsets of w including the empty set and w itself. Define V to be a family of subsets of $\mathbb{Z}_n$, specifically let V represent the maximum independent sets in G_b meaning that, for $v \subset Z_n = \{0, 1, \ldots, n-1\}$, $v \in V$ iff v is an independent set in G_b and there does not exist a v' which is an independent set in G_b such that $v \subset v'$, $v \neq v'$. Then G_b specifies V precisely and V specifies G_b precisely. For instance, for $n = 6$ let G_b be defined by the adjacency matrix $\Gamma = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$.

Then $V = \{\{0, 1, 2\}, \{2, 3, 4\}, \{1, 2, 3, 5\}\}$. Observe that V also lists the maximum cliques in the graph complement, $\overline{G_b}$ of G_b. From V we can compute those row subsets of $\mathcal{A}^T$ whose product is independent of product order, i.e. the row subsets that are fully commutative. We call this set of subsets $\mathcal{E}(V)$ and a member of $\mathcal{E}(V)$ represents a unique member of $S^\perp$ with a $+1$ coefficient. For our example there are $|\mathcal{E}(V)| = 24$ such row subsets, namely

$$\begin{aligned} \mathcal{E}(V) = \quad &\{\emptyset, \{0\}, \{1\}, \{0, 1\}, \{2\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}, \\ &\{3\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}, \{4\}, \{2, 4\}, \{3, 4\}, \{2, 3, 4\}, \\ &\{5\}, \{1, 5\}, \{2, 5\}, \{1, 2, 5\}, \{3, 5\}, \{1, 3, 5\}, \{2, 3, 5\}, \{1, 2, 3, 5\}\}. \end{aligned}$$

Then $\overline{\mathcal{E}(V)} = \mathcal{P}(\mathbb{Z}_n) \setminus \mathcal{E}(V)$ is the family of subsets of $\mathbb{Z}_n$ that represent non-commuting row subsets of $\mathcal{A}^T$, i.e. a member of $\overline{\mathcal{E}(V)}$ represents a unique member of $S^\perp$ with a ± 1

coefficient. The number of them is $|\overline{\mathcal{E}(V)}| = 2^n - |\mathcal{E}(V)|$, this being the number of members of $S^\perp$ with a ± 1 coefficient. For our example $|\overline{\mathcal{E}(V)}| = 2^6 - 24 = 40$. We can express $\mathcal{E}$ in terms of power sets as follows,

$$\mathcal{E}(V) = \bigcup_{w \in V} \mathcal{P}(w).$$

We now provide a recursive algorithm to compute $\mathcal{E}(V)$, given $\mathcal{A}^T$ (and therefore V). Let $w \subset \mathbb{Z}_n$, $\hat{V} = \bigcup_{w,w' \in V, w \neq w'} w \cap w'$ and, for $w \in V$, let $V_w = \bigcup_{w' \in V \setminus w} w \cap w'$. For our example, $V = \{\{0,1,2\}, \{2,3,4\}, \{1,2,3,5\}\}$, $\hat{V} = \{\{0,1,2\} \cap \{2,3,4\}, \{0,1,2\} \cap \{1,2,3,5\}, \{2,3,4\} \cap \{1,2,3,5\}\} = \{\{2\}, \{1,2\}, \{2,3\}\}$ and $V_{\{0,1,2\}} = \{\{0,1,2\} \cap \{2,3,4\}, \{0,1,2\} \cap \{1,2,3,5\}\} = \{\{2\}, \{1,2\}\}$. Then, recursively,

$$\mathcal{E}(V) = \mathcal{E}(\hat{V}) \cup \bigcup_{w \in V} \mathcal{P}(w) \setminus \mathcal{E}(V_w).$$

So, for our example with $V = \{\{0,1,2\}, \{2,3,4\}, \{1,2,3,5\}\}$ we obtain

$$
\begin{aligned}
\mathcal{E}(\hat{V}) =\ & \mathcal{E}(\{\{2\},\{1,2\},\{2,3\}\}) \cup \mathcal{P}(\{0,1,2\}) \setminus \mathcal{E}(\{\{2\},\{1,2\}\}) \\
& \cup\ \mathcal{P}(\{2,3,4\}) \setminus \mathcal{E}(\{\{2\},\{2,3\}\}) \cup \mathcal{P}(\{1,2,3,5\}) \setminus \mathcal{E}(\{\{1,2\},\{2,3\}\}) \\
=\ & \mathcal{E}(\{\{1,2\},\{2,3\}\}) \cup \mathcal{P}(\{0,1,2\}) \setminus \mathcal{P}(\{1,2\}) \\
& \cup\ \mathcal{P}(\{2,3,4\}) \setminus \mathcal{P}(\{2,3\}) \cup \mathcal{P}(\{1,2,3,5\}) \setminus \mathcal{E}(\{\{1,2\},\{2,3\}\}) \\
=\ & \{\{0\},\{0,1\},\{0,2\},\{0,1,2\}\} \cup \{\{4\},\{2,4\},\{3,4\},\{2,3,4\}\} \cup \mathcal{P}(\{1,2,3,5\}),
\end{aligned}
$$

from which we obtain the family of 24 sets written above.

8 Appendix B

8.1 $e = 1$ qubit extensions

We consider here the simplest case where $e = \frac{1}{2}\mathrm{rank}(\Gamma) = 1$.

Lemma 16 *Let j be a vertex of the mixed graph described by A, for which $e = 1$, such that vertex j is either disconnected or connected to other vertices only via undirected edges. Then $\mathcal{A}^e_{j,n} = I$.*

Proof.   From the conditions in the lemma, row j of $\mathcal{A}$ commutes with all other rows in $\mathcal{A}$. As $e = 1$ then there are at least two other rows of $\mathcal{A}$, rows h and k, such that $\mathcal{A}^e_{h,n} \neq \mathcal{A}^e_{k,n}$, $\mathcal{A}^e_{h,n}, \mathcal{A}^e_{k,n} \in \{X, Y, Z\}$. As we require row j of $\mathcal{A}^e$ to commute with rows h and k of $\mathcal{A}^e$ and, as row j of $\mathcal{A}$ commutes with rows h and k of $\mathcal{A}$, then the only choice for $\mathcal{A}^e_{j,n}$ is I. $\square$

A consequence of Lemma 16 is that, given a mixed graph described by A, we may immediately, and wlog, set all $\mathcal{A}^e_{j,n} = I$ for unconnected and undirected vertices j and focus on solving the extension problem for the residual directed graph comprising vertices involved in one or more directed edges. This is implicitly the case for Theorem 4 below.

Theorem 4 *Let $\mathcal{A}$ be an $n \times n$ Pauli stabilizer matrix such that, from (1), $e = 1$. Then $\mathcal{A}$ can always be extended to a fully-commuting stabilizer matrix, $\mathcal{A}^e$ of the form $\mathcal{A}^e = i^{I_{n+e} \star A^e} X^{I_{n+e}} Z^{A^e}$. Such a matrix stabilizes a graph state of $n + e = n + 1$ qubits, and has elements from $\{X, Y\}$ on the diagonal and elements from $\{I, Z\}$ off it.*

Proof.   (of Theorem 4)

Lemma 17 *For $\mathcal{A}^e = \left(\mathcal{A}^e_{i,j} \in \{I, X, Z, Y\}, 0 \leq i, j \leq n\right)$, we can wlog fix $\mathcal{A}^e_{n,n} = X$.*

Proof.   (of Lemma 17) If $\mathcal{A}^e_{n,n} = X$ then we are done. If $\mathcal{A}^e_{n,n} \in \{Z, Y\}$ then, by Lemma 3, we can conjugate $\mathcal{A}^e_{n,n}$ to X and, by Lemma 4, this leaves the density matrix stabilized by $\mathcal{A}$ unchanged, and preserves the pairwise commutation properties. If $\mathcal{A}^e_{n,n} = I$ then we multiply row n by any other row, j, where $\mathcal{A}^e_{j,n} \in \{X, Y, Z\}$, i.e. $\mathcal{A}^e_{n,n} \leftarrow \mathcal{A}^e_{j,n} \mathcal{A}^e_{n,n}$. At least one such row, j, must exist for $e \geq 1$. This operation preserves the codespace of $\mathcal{A}^e$, and results in $\mathcal{A}^e_{n,n} \in \{X, Y, Z\}$. Then we continue with conjugation if necessary, as discussed previously. $\qquad\square$

Although Lemma 17 restricts $\mathcal{A}^e_{n,n} = X$ we emphasise that there is nothing special about X here, we could've chosen to conjugate to Y or Z. But fixing to X simplifies the problem for us without costing anything in terms of generality, as, by Lemma 4, the associated density matrix is unchanged.

Lemma 18 *If the rows i and j of $\mathcal{A}$ are pairwise non-commuting then*

$$\mathcal{A}^e_{i,n}, \mathcal{A}^e_{j,n} \in \{X, Z, Y\}, \qquad \mathcal{A}^e_{i,n} \neq \mathcal{A}^e_{j,n}.$$

Proof.   (of Lemma 18) If rows i and j of $\mathcal{A}$, $i \neq j$, do not pairwise commute then, if $\mathcal{A}^e_{i,n} = \mathcal{A}^e_{j,n}$, or if $\mathcal{A}^e_{i,n}$ and/or $\mathcal{A}^e_{j,n}$ equals I, then rows i and j of $\mathcal{A}^e$ do not pairwise commute either. But we require $\mathcal{A}^e$ to be fully pairwise commuting. So $\mathcal{A}^e_{i,n} \neq \mathcal{A}^e_{j,n}$ and $\mathcal{A}^e_{i,n}, \mathcal{A}^e_{j,n} \in \{X, Z, Y\}$. $\qquad\square$

Lemma 19 *If the rows i and j of $\mathcal{A}$ are pairwise commuting then*

$$\mathcal{A}^e_{i,n} = \mathcal{A}^e_{j,n} \qquad or \qquad \text{at least one of } \mathcal{A}^e_{i,n} \text{ or } \mathcal{A}^e_{j,n} \text{ equals } I.$$

Proof.   (of Lemma 19) Rows i and j of $\mathcal{A}^e$ must pairwise commute and, if rows i and j of $\mathcal{A}$ pairwise commute, then matrices $\mathcal{A}^e_{i,n}$ and $\mathcal{A}^e_{j,n}$ must also pairwise commute, hence the conditions of the lemma. $\qquad\square$

Lemma 20 *Wlog, the elements $\mathcal{A}^e_{n,j}$, $0 \leq j < n$ can be restricted to elements from $\{I, Z\}$.*

Proof. (of Lemma 20) The last row, $\mathcal{A}_n^e = (\mathcal{A}_{n,j}^e, 0 \leq j \leq n)$, of $\mathcal{A}^e$, must pairwise commute with each of the n previous rows. We have, wlog, already fixed $\mathcal{A}_{n,n}^e = X$. We choose elements of $\mathcal{A}_{n,j}^e$, $0 \leq j < n$ from $\{I, X, Z, Y\}$. For each $\mathcal{A}_{n,j}^e \in \{X, Y\}$ we successively replace the nth row of $\mathcal{A}^e$, i.e. $\mathcal{A}_n^e$, with the product of rows j and n, i.e. $\mathcal{A}_n^e \to \mathcal{A}_j^e \mathcal{A}_n^e$ which ensures that, now, $\mathcal{A}_{n,j}^e \in \{I, Z\}$, and continue in this fashion until $\mathcal{A}_{n,j}^e \in \{I, Z\}$, $0 \leq j < n$. This process preserves the pairwise commuting property for the rows of $\mathcal{A}^e$. □

The row product operations of lemma 20 may change $\mathcal{A}_{n,n}^e = X$ to $\mathcal{A}_{n,n}^e \in \{Z, Y\}$ in which case, using Lemma 17, a further conjugation operation on the nth column of $\mathcal{A}^e$ is required to change $\mathcal{A}_{n,n}^e$ back to X. Note that, by Lemma 4, such an operation leaves unchanged the density matrix, ρ, described by $\mathcal{A}$.

At this point $\mathcal{A}^e$ has been transformed, by row operations and conjugation of the last column, to a matrix with X or Y on the diagonal, and with $\{I, Z\}$ off the diagonal, apart from the last column where $\mathcal{A}_{j,n}^e \in \{I, X, Y, Z\}$, $0 \leq j < n$, and $\mathcal{A}_{j,n}^e = X$. If $\mathcal{A}_{j,n}^e \in \{X, Y\}$ then we replace the jth row thus $\mathcal{A}_j^e \to \mathcal{A}_n^e \mathcal{A}_j^e$ so that, now, $\mathcal{A}_{j,n}^e \in \{I, Z\}$.

At this point $\mathcal{A}^e$ has been transformed, by row operations and conjugation of the last column, to a matrix with X or Y on the diagonal, and with $\{I, Z\}$ off the diagonal.

Lemma 21 $\mathcal{A}^e$ *is of the form* $\mathcal{A}^e = i^{I_{n+e} \star A^e} X^{I_{n+e}} Z^{A^e}$, *so must be a symmetric matrix.*

Proof. (of Lemma 21) All rows of $\mathcal{A}^e$ pairwise commute. Given that $\mathcal{A}^e$ has X or Y on the diagonal and $\{I, Z\}$ off the diagonal, then this is only possible if $\mathcal{A}^e$ is symmetric. □

Combining Lemmas 17, 18, 20, and 21, one arrives at the proof of Theorem 4. □

8.2 Conditions for G to have mixed rank $e = 1$

Remember that G is the mixed graph defined by adjacency matrix A, and G_b the undirected graph with adjacency matrix $\Gamma = A + A^T$.

Lemma 22 G *has mixed rank* $e = 1 \Leftrightarrow G_b$ *is a complete tripartite graph*[2], *with possible isolated vertices, and where one of the partitions can be empty (so that G_b is actually a complete bipartite graph).*

Proof. If (i, j) is an edge in G_b, then rows i and j of the stabilizer basis are anti-commuting so, by lemma 18, the corresponding elements in the extension column of $\mathcal{A}$, $(\mathcal{A}_{i,n}^e, \mathcal{A}_{j,n}^e)$ can only take the pairs (X, Z), (X, Y), (Z, X), (Z, Y), (Y, X), and (Y, Z). In other words the edge (i, j) in G_b forces vertices i and j to be associated with different operators in the extension column $\mathcal{A}_n^e$ - one can think of X, Z, Y as three colours. Therefore $e = 1$ is only possible if G_b is three-colourable, which implies that the graph is empty (1-coloured), bipartite (2-coloured) or tripartite (3-coloured). If $G_b = \emptyset$ then $rank(\Gamma) = 0$, so we discard this option. Isolated

---

[2]Thanks to Jon Eivind Vatne for useful discussions about graph theory.

vertices correspond to the rows that commute with all other rows, and can be extended by the column entry I, as seen in lemma 16. Let us now consider the connected part of G_b:

We are now going to prove that, if G has mixed rank $e = 1$, then the connected part of G_b is complete tripartite or complete bipartite, with possible isolated vertices; since it has to be 2- or 3-coloured, we have to prove that all the vertices on each partition are connected to all the vertices in the other partition(s). Consider any pair of vertices (u, v) such that u and v are in different partitions. The partitions are assigned two different colours/entries for the extension column, in the set $\{Z, X, Y\}$. [3] Therefore the rows u and v anti-commute, since the entries in the extension column anti-commute. Therefore there must be an edge between u and v in G_b, which proves that the graph is complete bipartite or complete tripartite.

We will now prove that if G_b is a complete bipartite or tripartite graph with possible isolated vertices, then G has mixed rank $e = 1$:

In general, the extension of G depends only on G_b: We have that $(u, v) \in G_b$ iff row u anti-commutes with row v. This is true because all unitaries U_j that form the stabilizer basis for a mixed graph state have exactly one X in position j, and Z and I in the other positions. If $(u, v) \in G_b$, we have in rows u and v the pair $X_u Z_v, I_u X_v$ ($u \to v$) or $X_u I_v, Z_u X_v$ ($u \leftarrow v$), and since all entries other than u and v commute (the set $\{Z, I\}$ is commutative), then row u anti-commutes with row v. On the other hand, if row u anti-commutes with row v, then one of the pairs $X_u Z_v, I_u X_v$ or $X_u I_v, Z_u X_v$ must be present in rows u and v, because as discussed all entries other than u and v commute, and these pairs correspond to $u \to v$ and $u \leftarrow v$, so $(u, v) \in G_b$. This means that the choice of the extension column/row will depend solely on G_b, since the only factor is the commutativity/anti-commutativity of the rows.

The extension of G by a node depends on whether we can extend the matrix by one column. We assign to each of the partitions the colours Z, X, Y. Since the graph is complete bipartite or tripartite, then any two nodes in the same partition get assigned the same colour/entry, and any two nodes in a different partition get assigned a different colour/entry. In particular, this means that there are no arrowed edges between any two nodes in the same partition, which means that their rows commute. Since they have the same extension entry, their extended rows also commute. This also means that there is an arrowed edge between any two nodes in different partitions, which means that their respective rows anti-commute. Since the extension entry is different for each of these two nodes, and is in the set $\{Z, X, Y\}$, this means that the extension rows now commute. This proves that one extension column is enough.

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

8.3   On parents and children for $e = 1$

In general, as we shall now show, for $e = 1$ we obtain (up to local equivalence) a maximum of three mixed states, obtained from a maximum of three parents (up to local equivalence), $|\psi_e\rangle$, as stabilized by $\mathcal{A}^e$.

---

[3]Note that I is not present because since it does not change the commutativity it can only be assigned to the rows that connect with any other rows (which correspond to isolated nodes on G_b), and we are considering here the connected part of G_b.

Lemma 23 *A maximum of 6 distinct children is possible when $e = 1$.*

Proof.   Isolated nodes in G_b have the extension I, so we consider only non-isolated nodes. If G_b is not connected then there are two or more non-empty subgraphs that are not connected to each other; however, then $rank(\Gamma) > 2$, which contradicts $e = 1$. This is because G_b is a nondirected graph for which any non-empty subgraph has rank at least 2, and the rank of G_b is the sum of the ranks of the unconnected subgraphs.

Lemma 22 states that G is at most 3-colourable if $e = 1$, as G_b is complete tripartite (or complete bipartite). G_b determines univocally whether two nodes have the same colour or not. There are 3 choices for the first colour, 2 for the second, and 1 for the remaining colour. In total that makes in principle 6 possible extension columns, yielding 6 different parents. Note that we only consider choices for $\mathcal{A}^e_{n,j}$, for $j = 0, \ldots, n-1$. The reason for this is that that, as shown previously, we can fix $\mathcal{A}^e_{n,n} = X$. $\square$

Lemma 24 *When $e = 1$ we obtain at most 3 local unitary inequivalent children.*

Proof.   Denote the resultant matrix after applying permutation $(Z\ Y)$ on $\mathcal{A}^e_{n,j}$, $j = 0, \ldots, n-1$, as $\mathcal{A}'^e_{n,j}$. The last rows of $\mathcal{A}$ and $\mathcal{A}'$ are equal. We can make both $\mathcal{A}$ and $\mathcal{A}'$ symmetric by multiplying by the last row the rows where the last column entry is X or Y. Thus the rows where $\mathcal{A}^e_{n,i} = X$ yield the same result as the rows where $\mathcal{A}'^e_{n,i} = X$, while we multiply the last row (which is equal in both matrices) by the rows where $\mathcal{A}^e_{n,j} = \mathcal{A}'^e_{n,k} = Y$. This means that $\mathcal{A}^e_{n,k} = \mathcal{A}'^e_{n,j} = Z$, so they do not get multiplied in their respective matrices. The effect of this is to complement the neighbourhood of node n, which comprises nodes j and k, and to induce the permutation $(X\ Y)$ in the diagonal position of these rows.

On the other hand, if we perform the local unitary operation $Z_K(DN)_n$, where $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $D = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ and $N = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$, and K is the largest set such that $\mathcal{A}^e_{n,k} = Z\ \forall k \in K$, the effect is the same as described above (see [5] for a description of the effect of N). This implies that of the 6 parents, only at most 3 are local unitary inequivalent. $\square$

We therefore obtain the following result.

Lemma 25 *Let $\mathcal{A}$ be such that, from (1), $e = 1$. Then $\mathcal{A}$ represents the mixed graph state*

$$\rho = \sum_{j=0}^{5} c_j \rho_j, \qquad \sum_{j=0}^{5} c_j = 1, \qquad c_j \geq 0, \forall j.$$

where $\rho_j = |\phi_{0,j}\rangle\langle\phi_{0,j}| + |\phi_{1,j}\rangle\langle\phi_{1,j}|$, $0 \leq j < 6$, are the six density matrices obtained from the six parents $|\psi^e_j\rangle$, as stabilized by $\mathcal{A}^e_j$.

Proof.   Follows immediately from lemma 23. $\square$

Although only at most 3 of them are locally inequivalent, we include them all in the general sum ρ, since changing ρ_j for a locally equivalent ρ'_j does not necessarily give local equivalence in ρ.

References

[1] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, H.-J. Briegel, "Entanglement in Graph States and its Applications", arXiv:quant-ph/0602096

[2] L.E. Danielsen, M. Parker, "On the Classification of All Self-Dual Additive Codes over GF(4) of Length up to 12", arXiv:math/0504522

[3] L. E. Danielsen, M. G. Parker, "Directed graph representation of half-rate additive codes over GF(4)", Des. Codes Cryptogr., Vol. 59, 1-3, April 2011.

[4] T.A. Brun, I. Devetak, M. H. Hsieh, "Correcting quantum errors with entanglement", Science 314 (2006), 436–439 (supporting material).

[5] C. Riera, "Spectral Properties of Boolean functions, Graphs and Graph States", Doctoral Thesis, submitted October, 2005, defended January 2006 - Universidad Complutense de Madrid.

[6] http://www.ee.pdx.edu/~mperkows/june2007/2005-q-0031-density-matrices-2.ppt